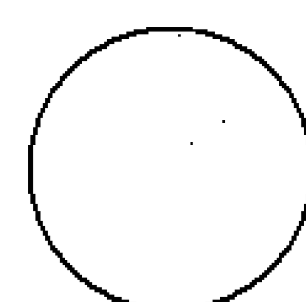
目　　录







第一章　初等计数函数

1.1. 排列与组合

1.1.1. 四种基本的排列组合问题

我们首先从一些简单的例子入手来说明排列和组合这两个基本概念.

问题 1.　有三个不同颜色的球 a, b, c, 每次取出二个排成一排,共有多少种排法?

容易得出,共有六种排法,它们是

$$ab, ac, ba, bc, ca, cb.$$

这里问题中的"排成一排"四个字意味着我们强调两个球的先后次序, 例如 ab 与 ba, 同样是由两个球 a 与 b 组成的, 但因次序不同,便看作是不同的排法.

问题 2.　有三个不同颜色的球 a, b, c, 每次取出二个构成一组,共有多少种取法?

这里"二个构成一组"意味着我们所关心的只是一个组由哪二个球组成,而不计较它们之间的次序. 对于问题 2 易见共有三种取法,即

$$\{a, b\}, \{a, c\}, \{b, c\}.$$

在上面的写法中 $\{a, b\}$ 也可以写作 $\{b, a\}$, 两者都表示由 a, b 两个球构成的那一组.

从这两个简单例子中,我们可以引出排列和组合的定义:

定义 1.　设 $\mathscr{A} = \{a_1, a_2, \cdots, a_m\}$ 是由 m 个不同元构



成的一个集合，则称自 $\mathscr{A}$ 中有序取出的 n 个元为 $\mathscr{A}$ 的一个 n-排列，而称由 $\mathscr{A}$ 中无序取出的 n 个元为 $\mathscr{A}$ 的一个 n-组合.

于是我们可以说，3 个不同的元可以构成 6 种 2-排列，3 种 2-组合.

问题 3. 有三个盒子甲、乙、丙，每个盒子中放着颜色相同的球，甲中为球 a，乙中为球 b，丙中为球 c. 现从这三个盒子中任意取出两个球排成一排，问有多少种不同的排法？

这里"任意取出"是指两个球既可取自不同的盒子，也可取自同一盒子，换言之构成一排的两个球可以是同一色的. 易见共有 9 种排法：

$$aa,\ ab,\ ac,\ ba,\ bb,\ bc,\ ca,\ cb,\ cc.$$

这种排列称作是"允许重复"的排列，问题中的"任意取出"还意味着我们对重复的次数不加限制. 同样，在"组合"的计算中也可以有重复. 由三种颜色的球构成的 2-组合，当允许重复时，共有 6 种取法，它们是

$$\{a, a\},\ \{b, b\},\ \{c, c\},\ \{a, b\},\ \{a, c\},\ \{b, c\}.$$

上面我们从四个简单的例子出发引出了四种最基本的排列组合问题. 下面我们转向一般情形的讨论.

命题 1. 由 m 个不同的元共可构成

$$[m]_n = m(m-1)(m-2)\cdots(m-n+1) \qquad (1)$$

种不同的 n-排列.

证. 从 m 个不同的元中顺序取出 n 个元时，头一个元可从 m 个元中任取其一，计有 m 种取法；头一个元选定后，第二个元可从剩下的 $m-1$ 个元中任选一个，计有 $(m-1)$ 种取法；…当选取最后一个元时，还剩下 $m-n+1$ 个元可供选择，故第 n 个元有 $(m-n+1)$ 种取法；因此顺序选出 n 个元共有 $m(m-1)(m-2)\cdots(m-n+1)$ 种方式.



公式(1)的一个重要的特殊情形是 $n=m$，此时 $[m]_n=[n]_n=n(n-1)(n-2)\cdots 2\cdot 1$ 即为 n 个不同的元排成一行的各种排列之总数. $[n]_n$ 一般记作 $n!$，读作"n 的阶乘"：

$$n!=n(n-1)(n-2)\cdots 2\cdot 1. \tag{2}$$

此外，我们约定 $0!=1$.

在计算机算法中，有时我们需要按照一定的法则，逐次产生全部 $n!$ 个排列. 迄今已有许多种生成全部排列的算法(见 Nijenhuis[118], Beckenbach[30])，其中最有效的算法是由 Johnson 与 Trotter 提出的. 在这一算法中，后一排列可从前一排列中交换两个相邻元的位置得出. 例如对 $n=4$，由此算法得出 $4!=24$ 种排列为

表 1.

1234	1342	4321	2431
1243	1324	3421	4231
1423	3124	3241	4213
4123	3142	3214	2413
4132	3412	2314	2143
1432	4312	2341	2134

这一算法在 1975 年为 Азагян 等所进一步简化(见 Азагян, Тамразян [26]).

图 1 表出了以表 1 所列 24 个排列为顶点的凸多面体. 两个排列若其一可由另一交换两个相邻元的位置得出时，在图 1 中便取为相邻两顶点. 用图论的术语来说，由上述算法顺序得出的诸排列相当于此凸多面体上诸顶点间的一条 Hamilton 迴路.

命题 2. 由 m 个不同的元共可构成 $[m]_n/n!$ 种 n-组合.

证. 由定义，n-组合与 n-排列之区别在于前者不计较元的先后顺序，因此由每个 n-组合可以作出 $n!$ 个不同的 n-排列. 于是若有 $C_{m,n}$ 种 n-组合，则 $C_{m,n}\cdot n!=[m]_n$，由此 $C_{m,n}=[m]_n/n!$.



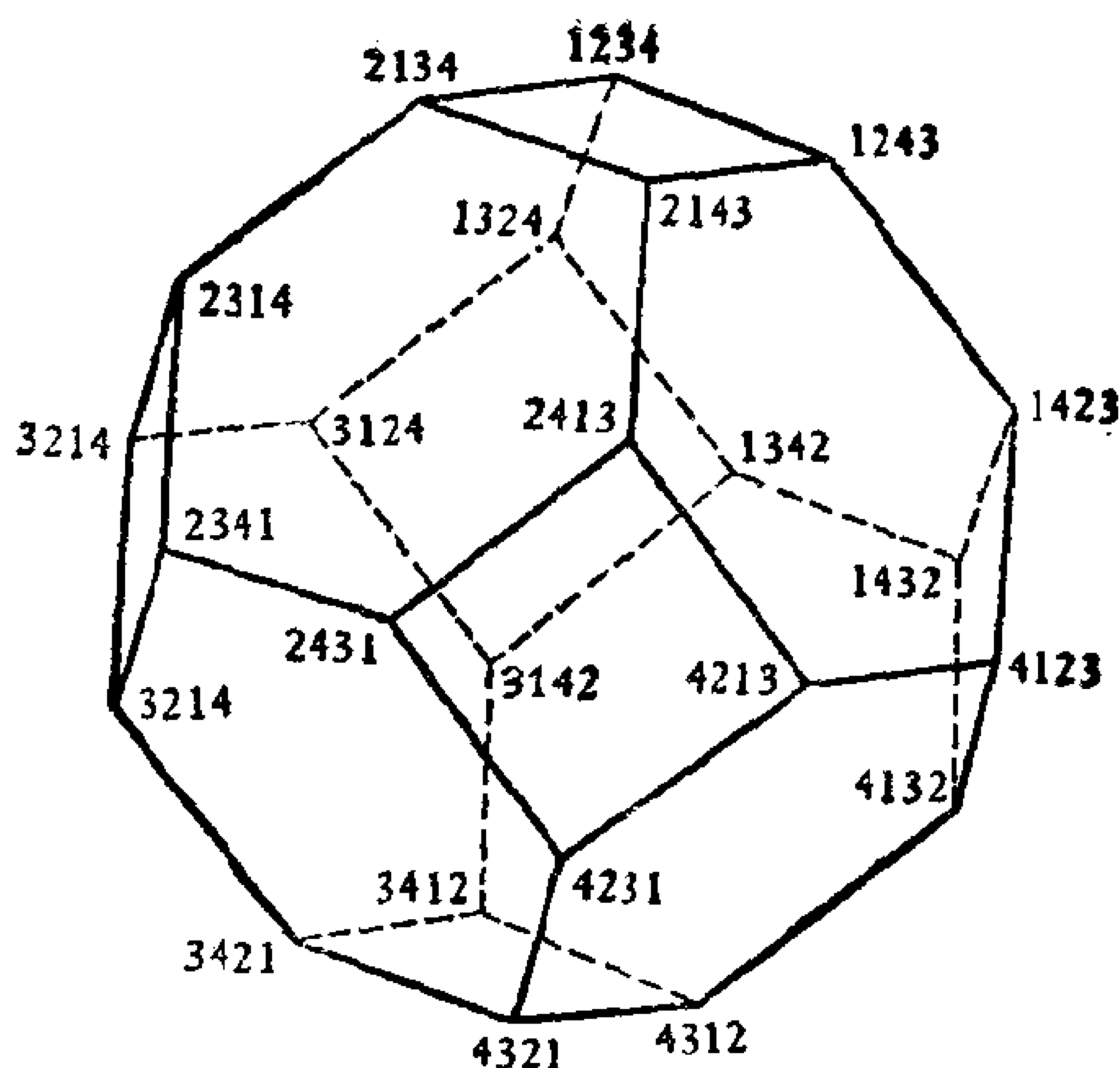


图 1． 由 24 个排列为顶点构成的凸多面体

$[m]_n/n!$ 一般记作 $\binom{m}{n}$.

$$\binom{m}{n} = m(m-1)(m-2)\cdots(m-n+1)/n! \tag{3}$$

称为二项式系数，在组合分析中占有重要地位，我们将在下一节中详加讨论。

命题 3. 由 m 种不同的元可作出的重复次数不限的 n-排列个数为 m^n.

证. 实际上，从 m 种不同的元有序取出 n 个元时，由于元的重复次数不限，每次选取时均有 m 种方式，于是共有 $m\times m\times\cdots\times m = m^n$ 种选取方式。

命题 4. 由 m 种不同的元可作出的重复次数不限的 n-组合个数为 $\binom{m+n-1}{n}$.

证. 今将 m 种不同的元用 $1, 2, \cdots, m$ 予以编号，于是每个允许重复的 n-组合具有形式 $\{a_1, a_2, \cdots, a_n\}$，其中



$a_1 \leqslant a_2 \leqslant \cdots \leqslant a_n$，因允许重复，其间等号可以成立。今将 $\{a_1, a_2, \cdots, a_n\}$ 对应于

$$\{a_1+0, a_2+1, \cdots, a_n+n-1\},$$

此种对应是双向单值的，亦即不同的 $\{a_1, a_2, \cdots, a_n\}$ 对应不同的 $\{a_1, a_2+1, \cdots, a_n+n-1\}$，反之亦然。但 $\{a_1, a_2+1, \cdots, a_n+n-1\}$ 显然是集合 $\{1, 2, \cdots, m, m+1, \cdots, m+n-1\}$ 的一个不带重复的 n-组合，故共有 $\binom{m+n-1}{n}$ 种。

在上述证明中，我们将带重复的组合计数问题转化为不带重复的组合计数问题，这种转换技巧在组合计数中经常遇到。下面试再举一例说明之。

问题 4. 一个 n 个元的集合 $\mathscr{A}$，共有多少个子集合？

例如当 $\mathscr{A}=\{a, b, c\}$ 时，它的子集合计有

$$\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}$$

共 8 个，其中 $\varnothing$ 表示不包含任何元的所谓"空集合"。

命题 5. 集合 $\mathscr{A}$ 的子集合个数为 $2^{|\mathscr{A}|}$，这里 $|\mathscr{A}|$ 表示集合 $\mathscr{A}$ 中元的个数。

证. 设 $\mathscr{A}=\{a_1, a_2, \cdots, a_n\}$. $\mathscr{A}$ 的每个子集合 $\{a_{i_1}, a_{i_2}, \cdots, a_{i_s}\}$ 与一个二元序列 $010\cdots011\cdots100$ 一一对应，其中在第 $i_1, i_2, \cdots, i_s$ 个位置上为 1，余为 0。而由命题 3，此种 n-排列的个数为 $2^n=2^{|\mathscr{A}|}$。

命题 3 也可以改述成另一种形式：一个 n 个元的排列 $a_1, a_2, \cdots, a_n$，若元 a_i 可取自集合 $\mathscr{A}$ 中任意一元，则全部排列个数为 $|\mathscr{A}|^n$。在这一陈述形式下，此命题显然可以推广成

命题 6. 一个 n 个元的排列 $a_1, a_2, \cdots, a_n$，若元 a_i 可取自集合 $\mathscr{A}_i$ 中任一元，则全部排列个数为 $|\mathscr{A}_1| \times |\mathscr{A}_2| \times$



$\cdots \times |\mathscr{A}_n|$.

用集合论记号，命题 6 也可写成

$$|\mathscr{A}_1 \times \mathscr{A}_2 \times \cdots \times \mathscr{A}_n| = |\mathscr{A}_1| \times |\mathscr{A}_2| \times \cdots \times |\mathscr{A}_n|. \tag{4}$$

式中 $\mathscr{A} = \mathscr{A}_1 \times \mathscr{A}_2 \times \cdots \times \mathscr{A}_n$ 表示诸集合 $\mathscr{A}_1, \cdots, \mathscr{A}_n$ 的直积，它由形如 $(a_1, a_2, \cdots, a_n)$，其中 $a_i \in \mathscr{A}_i$ 的元所组成.

1.1.2. 阶乘函数

在上一小节的讨论中我们引出了计数函数 $[m]_n$，通常我们称

$$[x]_n = x(x-1)(x-2)\cdots(x-n+1) \tag{5}$$

为下阶乘函数. 与之相应，我们定义上阶乘函数为

$$[x]^n = x(x+1)(x+2)\cdots(x+n-1). \tag{6}$$

下面的命题给出了上阶乘函数的组合学意义.

命题 7. 将 n 个不同的元，分放到 m 个不同的盒子中，每个盒子可容纳的元数不限，但必须计及放入时的先后次序(即所谓“有序的盒子”)，则共有 $[m]^n$ 种放法.

例如将元 $\{1, 2\}$ 分放到 2 个有序的盒子中，共有 $[2]^2 = 6$ 种放法：

$$\begin{array}{ccc} \varnothing|1,2 & 1|2 & 1,2|\varnothing \\ \varnothing|2,1 & 2|1 & 2,1|\varnothing \end{array}$$

证. 假定 n 个元有 T_n 种放法. 在 $n-1$ 个元的情形，每一种放法可以表示成

$$i_1 i_2 \cdots | i_k i_{k+1} \cdots | \cdots | \cdots i_{n-1}.$$

在这一排中有 $(n-1)+(m-1)$ 个记号(i_k 或 $|$)，于是将 i_n 放入时共有 $(n-1)+(m-1)+1$ 种方式，因此 $T_n = (m+n-1)T_{n-1}$，由此递推式即得 $T_n = [m]^n$.



同样，与 $[m]_n/n!$ 相应，我们给出 $[m]^n/n!$ 的组合学意义如下：

设 $\mathscr{A}$ 为由 m 个字母 $a_1, a_2, \cdots, a_m$ 所构成的一个有序集合，其次序为 $a_1 < a_2 < \cdots < a_m$. 一个由 $\mathscr{A}$ 中字母拼成的字 $x_1x_2\cdots x_n$，若满足条件 $x_1 \leqslant x_2 \leqslant \cdots \leqslant x_n$，则称为一个递增字. 例如对 $\mathscr{A} = \{a, b, c\}$, $a < b < c$. 长为 2 的递增字共有 6 个：

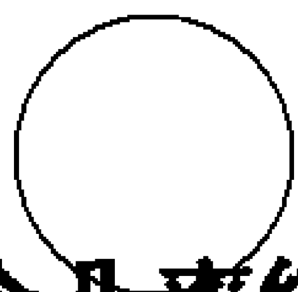
$$aa, ab, ac, bb, bc, cc.$$

命题 8. m 个字母 $a_1 < a_2 < \cdots < a_m$ 共可组成 $[m]^n/n!$ 个长为 n 的递增字.

证. n 个元在 m 个有序盒子中的每种分放方式均可对应一个递增字. 例如当 $m = 4$, $n = 7$ 时

$$\underbrace{|\ 3\ |}_{a_1}\quad \underbrace{|\ 251\ |}_{a_2}\quad \underbrace{|\qquad|}_{a_3}\quad \underbrace{|\ 647\ |}_{a_4} \longrightarrow a_1a_2a_2a_2a_4a_4a_4.$$

每种分放方式对应于一个且仅一个递增字，而对每个递增字计有 $n!$ 个不同的分放方式与之相应. 由此便可推出所述命题.



1.1.3. 两个几率统计问题

(i) (**Banach 火柴盒问题**，见 Feller[63]) 一个数学家，随身携带两个火柴盒，当他要用火柴时，随意从其中的一盒中取出一根. 假定开始时两个火柴盒中各有 n 根火柴，问在某一次该数学家发现拿出的那盒火柴已经用空时，另一盒中尚剩 $p(p < n)$ 根火柴的几率是多少？

解. 该数学家从开始使用两盒满的火柴起至发现所述情形止，共用去了 $2n - p$ 根火柴：$a_1, a_2, \cdots, a_{2n-p}$，其中 a_i 等于 A 或 B，表示第 i 根火柴取自盒子 A 或盒子 B. 此种排列显然有 2^{2n-p} 种(命题 3)，而欲出现所述情形，必须在 a_i 中



有 n 个 A 或 n 个 B，此种排列显然有 $2\binom{2n-p}{n}$ 个(命题 2)。因此所求几率等于

$$\binom{2n-p}{n}\Big/2^{2n-p-1}.$$

(ii) (**Boltzmann 分布**,见曹有祺[7]) 一个晶体体系由 n 个原子组成,其中有 n_1 个原子能级为 ε_1, n_2 个能级为 ε_2, $\cdots$. 每种能级 ε_i 又有 ω_i 种不同的量子状态,能级为 ε_i 的原子可以处于其中任一状态,问此种体系有多少种微观状态?

此问题相当于从 ω_1 种编了号的红球中取出 n_1 个(编号允许重复),从 ω_2 种编了号的黑球中取出 n_2 个,…将它们排成一排共有多少种方式? 例如 $n_1=\omega_1=2$, $n_2=\omega_2=1$ 时共有 12 种:

$$\begin{matrix} a_1a_1b & a_1ba_1 & ba_1a_1 \\ a_1a_2b & a_1ba_2 & ba_1a_2 \\ a_2a_1b & a_2ba_1 & ba_2a_1 \\ a_2a_2b & a_2ba_2 & ba_2a_2 \end{matrix}$$

为解决这一问题,我们首先注意到 n 个不同的球共有 $n!$ 种排列方式,如果同色球之间没有区别,则共有 $n!/n_1!n_2!\cdots$ 种排列,因为此相当于从 n 个位置中任意选出 n_1 个放红球,计有 $\binom{n}{n_1}$ 种.然后从 $n-n_1$ 个位置中选出 n_2 个放黑球,共有 $\binom{n-n_1}{n_2}$,$\cdots$故共有 $\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots=n!/n_1!n_2!\cdots$ 种. 但 n_1 个红球有 ω_1 种编号,且编号可以任取,故排列方式个数等于 ω_1 种元的可重复的 n_1-排列个数 $\omega_1^{n_1}$. 因此总的排列方式个数亦即体系的微观状态数为

$$L=(n!/n_1!n_2!\cdots)\omega_1^{n_1}\omega_2^{n_2}\cdots=n!\prod_i \omega_i^{n_i}/n_i. \quad (7)$$

对于一个体系而言它的总粒子个数 n 与总能量 ε 是确定的，亦即

$$\sum n_j = n,\ \sum n_j\varepsilon_j = \varepsilon. \tag{8}$$

试问哪一种分布 $n_1, n_2, \cdots$ 所给出的微观状态数 L 为最大？此问题归结为在条件 (8) 下求目标函数 L 之极大. 应用 Lagrange 乘子法可解出状态数最大的分布为

$$n_j^* = (n/\omega)\omega_j e^{-\beta\varepsilon_j},\ \omega = \sum\omega_j e^{-\beta\varepsilon_j},$$

其中 β 为常数. 此种分布在统计力学中称作 Boltzmann 分布.

本节讨论了几种简单但很基本的组合排列问题，在应用中我们会遇到一些更复杂的情形. 例如在排列计数中，我们可以对元的重复次数加上若干限制，对元的相邻关系或者位置提出某些要求；我们还可以考察环状的排列等等，这些问题的求解需要更多的技巧，我们将在以后各章中陆续讨论.

1.2. 二项式系数

1.2.1. 二项式定理

“二项式系数”的名称来自下面的二项式展开定理：

定理 A (二项式定理). 设 n 为非负整数，则

$$(1+x)^n = \sum \binom{n}{k} x^k \tag{1}$$

式中求和下标 k 遍及 0 至 n 的非负整数.

证. 因 $(1+x)^n = (1+x)(1+x)\cdots(1+x)$，在展开过程中，自 n 个括号 $(1+x)$ 中任选 k 个，取出 x，再从余下 $n-k$ 个括号中取出 1，便形成一个幂次 x^k，因此展开式中 x^k 前的系数即为 n 个元的 k-组合个数 $\binom{n}{k}$.



今将二项式系数 $\binom{n}{k}$ 排成下面的三角阵形式

$$
\begin{array}{ccccccccc}
 & & & & \binom{0}{0} & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots
\end{array}
\longrightarrow
\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots
\end{array}
$$

这一三角阵称为"**杨辉三角形**".我国早在十一世纪中叶,在宋朝的《黄帝九章算术细草》中就列出了这个三角阵,用于开任意高次方根,较之欧洲人的同一发现要早三百多年.

在讨论二项式系数的各种性质之前,我们首先将 $\binom{n}{k}$ 的定义范围予以适当扩大. 为此注意到表示式(1.1.3)[1]的右边实际上对任何实数 m 均有定义,因此对于任意实数 a,我们定义

$$\binom{a}{k} = a(a-1)\cdots(a-k+1)/k!. \tag{2}$$

由此定义特别可以推出

$$\binom{-n}{k} = (-1)^k \binom{n+k-1}{k}. \tag{3}$$

1) 式(1.1.3) 表示 1.1 节第(3)式,又如命题 (1.2.2) 表示 1.2 节命题 2,等等.



$$\binom{n}{n+m} = 0 \ (n = 0, 1, 2, \cdots; \ m = 1, 2, 3, \cdots). \quad (4)$$

此外我们约定

$$\binom{a}{0} = 1, \ \binom{a}{-m} = 0 \ (m = 1, 2, 3, \cdots). \quad (5)$$

利用上述诸式，便可将二项式系数 $\binom{n}{k}$ 的定义扩大到 n 为任意实数，k 为任意整数的情形. 在此种扩大了的定义下，由复变函数论的已知结果可以推出：二项式定理 (1) 对任意实数 n 成立，此时式中的求和下标 k 遍及所有整数，但当 n 不是非负整数时，要求变量 $|x| < 1$.

下面我们从二项式定理(1)入手，推导二项式系数的一些基本性质. 在下面诸等式中，若无特别说明，m, n, k, p 等均表示非负整数. 和式 $\sum_k$ 遍及所有非负整数 k.

1. 基本关系式

$$\binom{n}{k} = n!/k!(n-k)! \ (n \geqslant k). \quad (6)$$

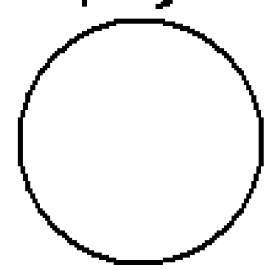
由此推出对称关系式

$$\binom{n}{k} = \binom{n}{n-k}. \quad (7)$$

2. 加法公式

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k} \ (\text{对任何整数 } k). \quad (8)$$

这一等式表示在杨辉三角形中，每个数等于它肩上的两个数之和.



3. 和式

$$\text{(i)} \ \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n. \quad (9)$$



(ii) $\binom{0}{m}+\binom{1}{m}+\cdots+\binom{n}{m}=\binom{n+1}{m+1}$. (10)

(iii) $\binom{n}{0}+\binom{n+1}{1}+\cdots+\binom{n+p}{p}$

$$=\binom{n+p+1}{p}. \tag{11}$$

(iv) $\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\cdots$

$$=\binom{n}{1}+\binom{n}{3}+\binom{n}{5}+\cdots=2^{n-1}. \tag{12}$$

(v) $\binom{n}{1}+\binom{n}{4}+\binom{n}{7}+\cdots$

$$=\frac{1}{3}\left(2^n+2\cos\frac{(n-2)\pi}{3}\right). \tag{13}$$

一般

(vi) $\binom{n}{k}+\binom{n}{m+k}+\binom{n}{2m+k}+\cdots$

$$=\frac{1}{m}\sum_{j=0}^{m-1}\left(2\cos\frac{j\pi}{m}\right)^n\cos\frac{j(n-2k)\pi}{m}. \tag{14}$$

4. 积之和

(i) $\sum_k\binom{n}{k}\binom{m}{p-k}=\binom{m+n}{p}$. (15)

(ii) $\sum_k\binom{n}{k}\binom{m}{p+k}=\binom{m+n}{p+n}$. (16)

(iii) $\sum_k\binom{n}{k}\binom{m-1}{k-1}=\binom{m+n-1}{n}$. (17)

(iv) $\sum_k(-1)^k\binom{k}{m}\binom{n}{k}=\delta_{mn}(-1)^m$. (18)



式中 δ_{mn} 为 Kronecker 符号：$m=n$ 时 $\delta_{mn}=1$，否则$=0$。上式之特例为

$$\text{(v)}\ \sum_k (-1)^k \binom{n}{k} = \delta_{n0}. \tag{19}$$

证. 1. 首先我们注意到当 n 为非负整数时，(1) 式的导出只利用了 $\binom{n}{k}$ 的组合学意义，因此我们完全可以自 (1) 式出发推证(6)式. 为此，只须在(1)式两边对 x 求导 k 次，然后令 $x=0$，即得 $n(n-1)\cdots(n-k+1)=\binom{n}{k}k!$，此即(6)式.

2. (8) 式可从 $(1+x)^n=(1+x)^{n-1}+x(1+x)^{n-1}$ 两边展开式中比较 x^k 前的系数得出.

3. (9) 式可在(1)式中取 $x=1$ 得出.

(10) 式可从等式

$$1+(1+x)+(1+x)^2+\cdots+(1+x)^n$$
$$=((1+x)^{n+1}-1)/x$$

比较两边 x^m 前系数得出.

(11) 式左边显然为 $x^p(1+x)^n+x^{p-1}(1+x)^{n-1}+\cdots+(1+x)^{n+p}$ 展开式中 x^p 前面的系数，将这一等比级数求和，得 $(1+x)^{n+p+1}-x^{p+1}(1+x)^n$，它的展开式中 x^p 前的系数显然为 $\binom{n+p+1}{n}$，故得 (11) 式.

(12) 式与(13)式均为(14)式的特例. 为证(14)式我们注意到：对于任一和式 $f(x)=\sum_k a_k x^k$，若以 ω 记 1 的 m 次根：$\omega=\exp\left(\frac{2\pi i}{m}\right)$，则对任二整数 $m>k\geqslant 0$，



$$a_kx^k + a_{k+m}x^{k+m} + a_{k+2m}x^{k+2m} + \cdots$$
$$= (1/m)\sum_{j=0}^{m-1} \omega^{-jk}f(\omega^j x).$$

令 $f(x)=(1+x)^n$，并注意到 $(1+\exp(2ai))^n = (2\cos a)^n\cdot \exp(nai)$，即证得(14)式.

4. (15) 式可从 $(1+x)^{m+n} = (1+x)^m(1+x)^n$ 两边比较 x^p 前系数得出.

(16) 式可从 $(1+(1/x))^n(1+x)^m = (1+x)^{n+m}/x$ 两边比较 x^p 前系数得出.

(17) 式可从 $(1+(1/x))^{n-1}(1+x)^m=(1+x)^{n+m-1}/x^{n-}$ 两边比较 x 前系数得出.

将 $(1+x)^n = \sum_k \binom{n}{k} x^k$ 两边对 x 微分 m 次，并除以 $m!$，即得

$$\binom{n}{m}(1+x)^{n-m} = \sum_k \binom{k}{m}\binom{n}{k}x^{k-m}.$$

令 $x=-1$ 即推出(18)式.

迄今，人们所发现的有关二项式系数的恒等式已有上千个，上面选列了最常用的 4 组. 读者可在 Gould[72] 中找到更多的关系式. 在上面诸式的证明中，我们运用了相同的推理方式，即均从二项式定理(1)入手. 这些关系式当然也可以从基本关系式(6)或(8)出发或者直接从 $\binom{n}{k}$ 的组合意义推出. 例如对于(10)式可应用加法公式(8)，证之如下：

$$\binom{0}{m}+\binom{1}{m}+\cdots+\binom{n}{m} = \binom{m}{m}$$
$$+\binom{m+1}{m}+\binom{m+2}{m}+\cdots+\binom{n}{m}$$



$$=\left(\binom{m+1}{m+1}+\binom{m+1}{m}\right)$$

$$+\binom{m+2}{m}+\cdots+\binom{n}{m}=\binom{m+2}{m+1}$$

$$+\binom{m+2}{m}+\cdots+\binom{n}{m}$$

$$=\binom{m+3}{m+1}+\cdots+\binom{n}{m}=\cdots$$

$$=\binom{n}{m+1}+\binom{n}{m}=\binom{n+1}{m+1}.$$

又如(15)式也可经下面的推理得出：考察n个元的集合 $\mathscr{A}$ 和m个元的集合 $\mathscr{B}$ 之并集 $\mathscr{A}\cup\mathscr{B}$，$\mathscr{A}\cup\mathscr{B}$ 共有 $m+n$ 个元，因此它的 p-组合个数等于$\binom{m+n}{p}$. 但另一方面每个这样的组合无非是由从 $\mathscr{A}$ 中取出k个元，再从 $\mathscr{B}$ 中取出 $p-k$ 个元组成，因而共有$\binom{n}{k}\binom{m}{p-k}$种取法，令$k$遍及 0 到 p，即得证(15)式.

我们在证明中之所以都从(1)式入手，目的是强调一下下一章中将详加说明的生成函数方法. 事实上，有些等式如(14)，若直接从$\binom{n}{k}$的组合学意义或基本关系式(6)出发求证要困难得多.

1.2.2. 二项式系数之推广

1. 多项式系数. 注意到二项式基本定理(1)也可表述成：若n为非负整数，则



$$(x+y)^n=\sum_k \binom{n}{k} x^k y^{n-k}. \qquad (20)$$

将变元 x, y 的个数增多，即得到下面的

定理 B (多项式定理). 若 n 为非负整数，则

$$(x_1+x_2+\cdots+x_p)^m=\sum_{\substack{n_1,n_2,\cdots,n_p\geqslant 0\\ n_1+n_2+\cdots+n_p=m}} \times \binom{n}{n_1, n_2, \cdots, n_p} x_1^{n_1}x_2^{n_2}\cdots x_p^{n_p}. \qquad (21)$$

其中

$$\binom{n}{n_1, n_2, \cdots, n_p}=\frac{n!}{n_1!n_2!\cdots n_p!} \qquad (22)$$

称作多项式系数.

为证明(22)式，只须在(21)式两边施以微分算子 $\partial^n/\partial x_1^{n_1}\partial x_2^{n_2}\cdots\partial x_p^{n_p}$, 并令 $x=0$, 便得

$$n!=\binom{n}{n_1, n_2, \cdots, n_p} n_1!n_2!\cdots n_p!.$$

由此便推出(22)式.

多项式系数的组合学意义如下:

命题 1. 将 n 个不同的元分放在 p 个盒子 $T_1, \cdots, T_p$ 中，在 T_1 中放 n_1 个，在 T_2 中放 n_2 个，…, T_p 中放 n_p 个，而 $\sum n_i=n$, 在同一盒子中元之间的次序不计，则共有 $\binom{n}{n_1, \cdots, n_p}$ 种放法.

证. 见 1.2.3 节中问题 2 之解.

命题 2. 将 n_1 个白球，n_2 个黑球，…，n_p 个红球排成一排，假设同色球之间毫无区别，则共有 $\binom{n_1+n_2+\cdots+n_p}{n_1, n_2, \cdots, n_p}$ 种排法.



证．同上．

2. Gauss 二项式系数． 所谓 Gauss 二项式系数是指

$$\binom{n}{k}_q=\frac{(1-q^n)(1-q^{n-1})\cdots(1-q^{n-k+1})}{(1-q^k)(1-q^{k-1})\cdots(1-q)}. \qquad (23)$$

若将上式右边的分子分母约去公因子 $(1-q)^k$，然后令 $q=1$，即见 $\lim\limits_{q\to 1}\binom{n}{k}_q=\binom{n}{k}$．亦即二项式系数 $\binom{n}{k}$ 可以看作 Gauss 二项式系数在 $q=1$ 时的特例．

Gauss 二项式系数出现于有限几何等问题的研究中．若 q 为某个素数的幂 $q=p^r$，则 $\binom{n}{k}_q$ 的组合学意义是：它表示有限域 $GF(q)$ 上 n 维向量空间的 k 维子空间的个数（见万哲先等[1]）．对于 Gauss 二项式系数亦成立的有一系列与通常二项式系数相仿的等式，例如

$$\binom{n}{k}_q=\binom{n-1}{k-1}_q+q^k\binom{n-1}{k}_q. \qquad (24)$$

此式当 $q=1$ 时即化作二项式系数的加法公式(8)．由(24)可见，$\binom{n}{k}_q$ 可表示成 q 的多项式，此种多项式通常称作 **Gauss 多项式**，由此可以引出所谓 **Gauss 和**，常见于一些数论问题的应用中（见 Rademacher [130]）．

3．二项式系数的另一种推广方式是将 k 的定义域推广到任意的实数．为此可利用函数 $\Gamma(x)=\int_0^\infty e^{-sx}s^{x+1}ds$ 与函数 $B(x,y)=\int_0^1 s^x(1-s)^y ds$ 间的关系式 $B(x,y)=\Gamma(x)\Gamma(y)/\Gamma\cdot(x+y)$，并注意到 $\binom{x+y}{y}=(x+y)!/x!y!$ 及 $\Gamma(n+$



1) $= n!$，即可用 $B(k, n-k+1)^{-1}$ 作为 $\binom{n}{k}$ 在任意实数 n，k 情形时的定义。

1.2.3. Shannon 不等式，二项式系数的数论性质

在组合计数方法的应用中，我们还会遇到有关二项式系数的其它结果。作为例子，我们给出有名的 Shannon 不等式和 Lucas 定理，它们在信息论和纠错编码中有着重要应用。

Shannon 不等式. 设 l 与 n 为非负整数，且 $l \leqslant \frac{n}{2}$，则

$$\sum_{i=0}^{l} \binom{n}{i} \leqslant 2^{nH(l/n)}. \tag{25}$$

其中 $H(p) = -p\log_2 p - (1-p)\log_2(1-p)$。

证. (Park [123]) 记

$$A(n, l) = \sum_{i=0}^{l} \binom{n}{i},$$

$$B(n, l) = 2^{nH(l/n)} = (n/l)^l (n/(n-l))^{n-l}.$$

因 $A(n, 0) = B(n, 0) = 1$，$A(2l, l) < A(2l, 2l) = 2^{2l} = B(2l, l)$，故(25)式当 $(n, l) = (n, 0)$ 及 $(2l, l)$ 时为真。为完成对 $l \leqslant n/2$ 的归纳证明，只须证明：若 (25) 式对 (n, l) 及 $(n, l+1)$ 为真，则对 $(n+1, l+1)$ 也真。事实上，若将(25)式记作命题 $S(n, l)$，并将之排成如杨辉三角形的形式，则显然可见：除去 $S(n, 0)$ 及 $S(2l, l)$ 外，余下的 $S(n, l)$ 之正确性可从它肩上的两个命题之正确性推出。现从命题 $S(n, l)$ 及 $S(n, l+1)$ 推证 $S(n+1, l+1)$。由加法公式(8)可见

$$A(n+1, l+1) = A(n, l+1) + A(n, l).$$



故由归纳假设

$$A(n+1, l+1) \leqslant B(n+1, l+1)(\alpha+\beta).$$

其中

$$\begin{aligned}\alpha &= B(n, l+1)/B(n+1, l+1) \\ &= (n/(n+1))^n((n-l)/(n-l-1))^{n-l-1}((n-l)/(n+1)), \\ \beta &= B(n, l)/B(n+1, l+1) \\ &= (n/(n+1))^n((l+1)/l)^l((l+1)/(n+1)).\end{aligned}$$

我们只须证明 $\alpha+\beta \leqslant 1$. 为此在上面两式之两边取对数，并注意到 $\log x \leqslant x-1$，即得

$$\log\alpha \leqslant -l/(n+1), \quad \log\beta \leqslant -(n-l-1)/(n+1).$$

故

$$\alpha+\beta \leqslant (e^{-(n-l-1)} + e^{-l})^{1/(n+1)}.$$

但当 $1 \leqslant l \leqslant n-2$ 时，$n-l-1 \geqslant 1$，$l \geqslant 1$，由此 $e^{-(n-l-1)} + e^{-l} \leqslant 2e^{-1} < 1$，证毕.

在不等式(25)中出现的函数 $H(p)$ 称作**熵函数**，是信息论中用以度量信息量的一个重要函数. Shannon 曾以上述不等式(25)为工具导出了有名的信息论基本定理(见 Feinstein [62]).

下面的 Lucas 定理描述了 $\binom{n}{k}$ 的数论性质.

Lucas 定理. 设 p 为素数，$n=\sum n_i p^i$，$k=\sum k_i p^i$ 为 n 与 k 的 p 进制展开，则

$$\binom{n}{k} \equiv \prod_i \binom{n_i}{k_i} \pmod{p}. \tag{26}$$

证. 首先我们注意到当 $p>k$ 时，$\binom{p}{k}=p(p-1)\cdots(p-k+1)/k!$ 为正整数，因此 $k!$ 除尽 $p(p-1)\cdots(p-k+1)$. 但 p 为素数，$k<p$，因此 $k!$ 除尽 $(p-1)(p-$



$2)\cdots(p-k+1)$. 由此可见 $\binom{p}{k}$ 有因子 p，此即当 $p>k$ 时，$\binom{p}{k}\equiv 0\ (\bmod p)$. 于是 $(1+x)^p\equiv 1+x^p\ (\bmod p)$. 由此

$$(1+x)^n=\prod_i (1+x)^{n_i p^i}$$
$$\equiv\prod_i (1+x^{p^i})^{n_i}\ (\bmod p).$$

此式右边之展开式中 x^k 前的系数显然为 $\binom{n_0}{k_0}\binom{n_1}{k_1}\binom{n_2}{k_2}\cdots$.

在纠错编码理论中常用 $p=2$ 时的 Lucas 定理，在这一特殊情形，Lucas 定理可以改述如下：
对任一非负整数 $n=\sum n_i 2^i$, $n_i=0$ 或 1, 记 $E(n)=\{i\,|\,n_i\neq 0\}$，则有

Lucas 定理 a. $\binom{n}{k}$ 为奇数当且仅当 $E(k)\subset E(n)$.

这一定理易推广到多项式系数的情形：

Lucas 定理 b. $\binom{n}{k_1,k_2,\cdots,k_r}$ 为奇数当且仅当 $E(k_i)\subset E(n)$ $(i=1,2,\cdots,r)$.

注及上述条件可改述成 $E(n)=\bigcup_i E(k_i)$, $E(k_i)\cap E(k_j)=\varnothing$ $(i\neq j)$. 亦即诸非空的 $E(k_i)$ 构成 $E(n)$ 的一个分划.

关于 Lucas 定理在纠错编码中的应用，可见 Berlekamp [37].

Lucas 定理给出了素数 p 除尽 $\binom{n}{k}$ 的一个简单的判别法



则，这一结果被 Singmaster[143] 加以推广，他研究了一个素数 p 的幂次可以除尽 $\binom{n}{k}$ 的条件以及 $\binom{n}{k}$ 的一些其他数论性质．例如他证得了：设 n, k 与 $n-k$ 的 p 进制展开式为 $n=\sum n_i p^i$，$k=\sum k_i p^i$ 及 $(n-k)=\sum r_i p^i$，则满足 $p^e \mid \binom{n}{k}$ 的最大整数 e 等于 $(1/(p-1))\sum(k_i+r_i-n_i)$．关于二项式系数的数论性质已有很多研究，例如 Albree[21]，Selmer [141] 等．

1.3. 三项递推式的一般解[1]

在本节中我们首先用二项式系数表出一个图论问题的

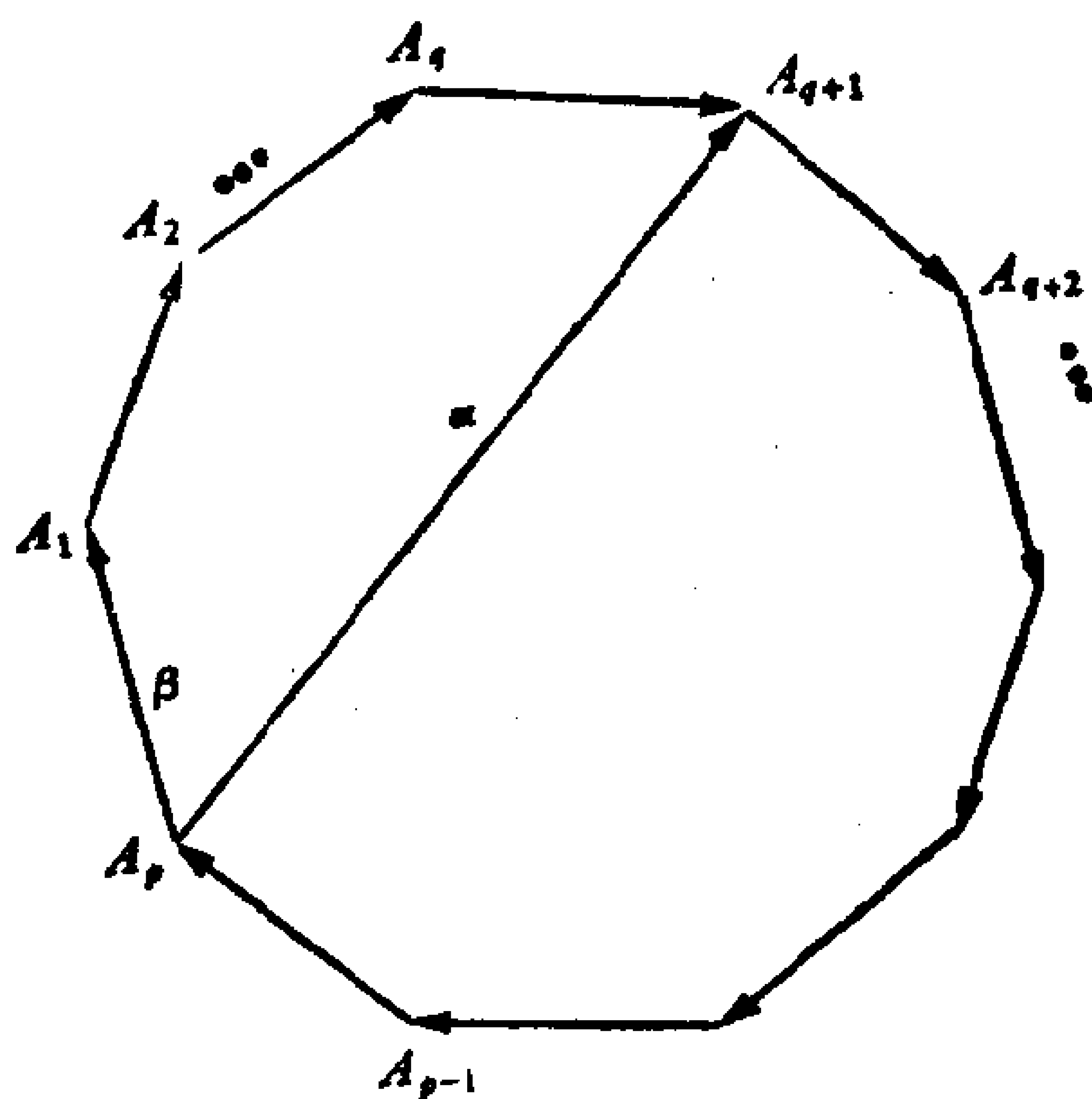


图 1.

1）不熟悉矩阵理论的读者可以跳过本节．



解，然后应用这一结果来导出三项递推式的一般解。

考察有向图 1，图中 p 个点 $A_1, \cdots, A_p$ 构成一个有向圈，另有一弧自 A_p 指向 A_{q+1}。问题是：自 A_i 出发回到 A_i 的长为 m 的闭路共有多少条？所谓一条路的长为 m 是指它由 m 条弧组成。

方向图 1 有两个有向圈，即大圈 $A_p \to A_1 \to A_2 \to \cdots \to A_{p-1} \to A_p$，长度为 p；小圈 $A_p \to A_{q+1} \to A_{q+2} \to \cdots \to A_p$，长度为 $p-q$。于是任一条自 A_1 出发回到 A_1 的闭路必定由若干个大圈及小圈组成。任取这样一条长为 m 的闭路，假设它由 x 个大圈，y 个小圈组成，则应有 $px+(p-q)y=m$。但这样的闭路因为出发点 A_1 位于大圈上，因此首先须绕大圈而行，于是每一条自 A_1 回到 A_1 的闭路必取形式：$A_1 \to A_2 \to \cdots \to A_{p-1} \to A_p \to A_i \to \cdots \to A_{p-1} \to A_p \to A_1$，其中 $A_p \to A_i \to \cdots \to A_p$ 部分系由 $x-1$ 个大圈及 y 个小圈组成，由于沿此 $x-1$ 个大圈及 y 个小圈的行走次序没有限制，因此共有 $\binom{x+y-1}{y}$ 种走法。于是自 A_1 至 A_1 的长为 m 的闭路共有

$$\sum_{\substack{x\geq 1, y\geq 0\\ px+(p-q)y=m}} \binom{x+y-1}{y}$$

条。当出发点取为 $A_2, \cdots, A_q$ 时情形显然与 A_1 相同。其次考察自 A_p 出发回到 A_p 的长为 m 的闭路。由于 A_p 同时位于大圈及小圈上，因此沿大圈与小圈的行走次序没有限制，于是长为 m 的闭路共有

$$\sum_{\substack{x, y\geq 0\\ px+(p-q)y=m}} \binom{x+y}{y}$$

条。在点 $A_{q+1}, \cdots, A_{p-1}$ 情形相同。



令若对一个由 x 个大圈及 y 个小圈组成的闭路加权，亦即对每一条这样的闭路赋以值 $\beta^x\alpha^y$，并称为该闭路的积，则由上面所作的分析易知命题 1 成立.

命题 1. 在有向图 1 中，自 A_i 出发回到 A_i 的所有长为 m 的闭路之积的累加和 S_i 等于

$$S_i = \sum_{\substack{px+(p-q)y=m \\ x\geqslant 1, y\geqslant 0}} \binom{x+y-1}{y} \beta^x\alpha^y$$

$$(i=1, 2, \cdots, q), \tag{1}$$

$$S_i = \sum_{\substack{px+(p-q)y=m \\ x, y\geqslant 0}} \binom{x+y}{y} \beta^x\alpha^y$$

$$(i=q+1, \cdots, p). \tag{2}$$

下面我们转向讨论三项递推式的求解. 在一些应用问题中，我们常需在初始条件 $a_0=c_0, a_1=c_1, \cdots, a_{p-1}=c_{p-1}$ 的条件下求解递推式

$$a_n=\alpha_1 a_{n-1}+\alpha_2 a_{n-2}+\cdots+\alpha_p a_{n-p}, \tag{3}$$

其中 α_i 与 p 及 n 均无关. 此种递推式的一般解法是令 $a_n=\lambda^n$，代入后即得特征方程

$$\lambda^p=\alpha_1\lambda^{p-1}+\alpha_2\lambda^{p-2}+\cdots+\alpha_{p-1}\lambda+\alpha_p. \tag{4}$$

若其中 p 个根 λ_i 互异，则(3)的一般解即为 $a_n=\sum_{i=1}^{p} d_i\lambda_i^n$. 为了确定常数 $d_1, \cdots, d_p$，还须求解 p 阶线性方程 $c_k=\sum_i d_i\lambda_i^k$ $(k=0, 1, \cdots, p-1)$. 当 p 个根中有重根时，情形就更繁杂. 当 $p\geqslant 5$ 时，由于高次代数方程没有一般的求根公式，因此由这条途径一般得不到解的明显表示式. 下面我们指出，利用命题 1 可将三项递推式

$$\begin{cases} a_{n+p}=\alpha a_{n+q}+\beta a_n, \\ a_0=c_0, \ a_1=c_1, \ \cdots, \ a_{p-1}=c_{p-1} \end{cases} \tag{5}$$



的解写成明显的形式，而且初始常数 $c_0, \cdots, c_{p-1}$ 显含于解的表示式中，从而避免了求解 p 阶线性方程组.

递推式(5)的特征方程为

$$\lambda^p - \alpha\lambda^q - \beta = 0. \tag{6}$$

与此方程相关的 Frobenius 矩阵为

$$F = (f_{ij}) = \begin{bmatrix} 0 & 1 & 0 \cdots 0 \cdots 0 \\ 0 & 0 & 1 \cdots 0 \cdots 0 \\ & & \ddots \\ & & \quad 1 \\ & & \quad\quad \ddots \\ 0 & 0 & 0 \cdots 0 \cdots 1 \\ \beta & 0 & 0 \cdots \alpha \cdots 0 \end{bmatrix},$$

其中 $\beta = f_{p1}$，$\alpha = f_{p,q+1}$，该阵的特征方程即(6). 既然每一矩阵必满足它的特征方程，于是

$$F^p = \alpha F^q + \beta I, \tag{7}$$

其中 I 为 p 阶单位阵. 若取 $C = (c_0, c_1, \cdots, c_{p-1})^T$，其分量由初始值 c_i 构成，并记 $F^m C = (a^{(m)}, \cdots)$，则由(7)式可见，$a^{(n+p)} = \alpha a^{(n+q)} + \beta a^{(n)}$，亦即 $a^{(m)}$ 满足递推式及初始条件(5). 因此，若 $F^{(m)} = (f_{ij}^{(m)})$，则(5)的解可表为

$$a^{(m)} = c_0 f_{11}^{(m)} + c_1 f_{12}^{(m)} + \cdots + c_{p-1} f_{1p}^{(m)}.$$

今阵 F 的方向图即图 1. 图中每一有向弧 $A_i \to A_j$ 对应于阵 F 的非零元 f_{ij}. 由矩阵乘法的定义易见矩阵 F 的幂次 F^m 中元 $f_{ij}^{(m)}$ 等于图 1 中所有从 A_i 到 A_j 的长度为 m 的路之积的累加和. 另外由(7)式易见 $f_{ij}^{(m)} = f_{jj}^{(m+i-j)}$，故利用命题 1 即可推出

定理 A 递推式(5)的一般解为

$$a_m = \sum_{j=0}^{q-1} c_j \beta f^{(m-p-j)} + \sum_{j=q}^{p-1} c_j f^{(m-j)},$$

其中 $f^{(-p)} = 1$，$f^{(m)} = 0\ (-p < m < 0)$，及



$$f^{(m)} = \sum_{\substack{px+(p-q)y=m \\ x,y\geq 0}} \binom{x+y}{y} \beta^x \alpha^y \quad (m \geq 0).$$

定理中的 $f^{(m)}$ 表示式若引用不定方程非负解理论（见闵嗣鹤，严士健[6]），可以写成更明显的形式．下面我们仅列出最后结果，中间的推导从略．

设 p 与 q 互素（一般情形容易转化成此种情形），且有连分式展开

$$\frac{p}{p-q} = k_1 + \cfrac{1}{k_2 + \cfrac{1}{k_3 + \cfrac{}{\ddots + \cfrac{1}{k_r}}}} = (k_1, k_2, \cdots, k_r),$$

则当 r 为偶数时

$$f^{(m)} = D\left(\frac{m\langle k_1, \cdots, k_{r-1}\rangle}{p}\right)\beta^{u+(p-q)} + \sum_{k=0}^{u/(p-q)} \binom{u+v+kq}{u-k(p-q)} \beta^{u-k(p-q)} \alpha^{v+kp},$$

其中

$$u = \langle k_2, \cdots, k_{r-1}\rangle m - (p-q)\left(\left[m\frac{\langle k_1, \cdots, k_{r-1}\rangle}{p}\right]+1\right),$$

$$v = -\langle k_1, \cdots, k_{r-1}\rangle m + p\left(\left[m\frac{\langle k_1, \cdots, k_{r-1}\rangle}{p}\right]+1\right).$$

当 r 为奇数时

$$f^{(m)} = D\left(\frac{m\langle k_2, \cdots, k_{r-1}\rangle}{p-q}\right)\alpha^{v+p}$$



$$+\sum_{k=0}^{[v/p]}\binom{u+v-kq}{v-kp}\beta^{u+k(p-q)}\alpha^{v-kp},$$

其中

$$u=-\langle k_2,\cdots,k_{r-1}\rangle m+(p-q)\left(\left[\frac{m\langle k_2,\cdots,k_{r-1}\rangle}{p-q}\right]+1\right),$$

$$v=\langle k_1,\cdots,k_{r-1}\rangle m-p\left(\left[\frac{m\langle k_2,\cdots,k_{r-1}\rangle}{p-q}\right]+1\right).$$

式中 $D(x)$ 定义为：若 x 为整数，$D(x)=1$；否则 $D(x)=0$。$[x]$ 表示 x 的整数部分，而 $\langle q_1,\cdots,q_l\rangle$ 表示 **Euler 括号**：

$$\langle q_1\rangle=q_1,\ \langle q_1,q_2\rangle=q_1q_2+1,\ \cdots,$$

$$\langle q_1,\cdots,q_l\rangle=q_l\langle q_1,\cdots,q_{l-1}\rangle+\langle q_1,\cdots,q_{l-2}\rangle.$$

它可以用下面的表格很方便地算出

	q_1	q_2	$\cdots$	q_{l-2}	q_{l-1}	q_l
						‖
1	q_1	$\langle q_1,q_2\rangle$	$\cdots$	$\langle q_1,\cdots,q_{l-2}\rangle+$	$\langle q_1,\cdots,q_{l-1}\rangle$	$\langle q_1,\cdots,q_l\rangle$

作为特例取 $p=2$，即可推出二阶递推式

$$\begin{cases}a_{n+2}=\alpha a_{n+1}+\beta a_n,\\ a_0=c_0,\ a_1=c_1\end{cases}$$

的一般解为

$$a_{2m}=c_0\sum_{i=-1}^{m-2}\binom{m+i}{2i+2}\beta^{m-i-1}\alpha^{2i+2}+c_1\sum_{i=0}^{m-1}\binom{m+i}{2i+1}\beta^{m-i-1}\alpha^{2i+1},$$

$$a_{2m+1}=c_0\sum_{i=0}^{m-1}\binom{m+i}{2i+1}\beta^{m-i}\alpha^{2i+1}$$

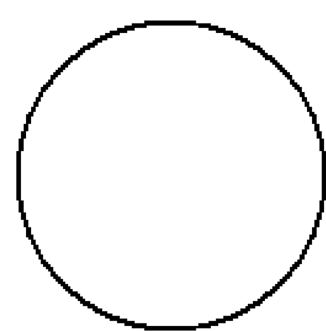




$$+c_1\sum_{i=-1}^{m-1}\binom{m+i+1}{2i+2}\beta^{m-i-1}\alpha^{2i+2}.$$

在上式中取 $c_0=c_1=\alpha=\beta=1$，即得有名的 Fibonacci 数列，$F_0=F_1=1$，$F_{n+2}=F_{n+1}+F_n$，由上式可见

$$F_{2m}=\sum_{i=0}^{m}\binom{m+i}{2i},\quad F_{2m+1}=\sum_{i=0}^{m}\binom{m+i+1}{2i+1}. \tag{8}$$



第二章　生成函数方法

2.1. Fibonacci 数与优选法

在 1.2 节中我们从 $(1+x)^n=\sum\binom{n}{k}x^k$ 出发推证了二项式系数的一系列等式．这种将数列 $\binom{n}{k}$ 与函数 $\sum\binom{n}{k}\cdot x^k=(1+x)^n$ 联系起来的作法称作“生成函数方法”．函数 $(1+x)^n$ 即称为 $\binom{n}{k}$ 的生成函数,因为将 $(1+x)^n$ 展开我们可以得到所有的 $\binom{n}{k}$． 一般,我们称 $f(x)=\sum a_kx^k$ 为数列 $a_0, a_1, a_2, \cdots$ 的生成函数,这一级数可以是有穷，也可以是无穷的． 运用生成函数方法，使我们能够通过对单个函数 $f(x)=\sum a_kx^k$ 的研究导出有关整个数列 a_k 的很多性质.这一方法是 Laplace 为解决几率问题首先引进的，它是组合计数中的一个很有效的方法．

本节我们将以 Fibonacci 数列为例说明生成函数方法,一般性的叙述将在下一节中给出．

Fibonacci 数列定义为

$$F_0=F_1=1,\ F_{n+2}=F_{n+1}+F_n,\ (n\geqslant 0)$$

它的头几项为

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \cdots\cdots.$$

这一数列以十三世纪意大利数学家 Fibonacci 的名字命名，在





最优搜索等问题中有着重要的应用．今首先求出它的生成函数 $F(x)=\sum_{n=0}^{\infty}F_nx^n$.

$$
\begin{aligned}
F(x) &= 1+x+\sum_{n=2}^{\infty}F_nx^n \\
&= 1+x+\sum_{n=2}^{\infty}(F_{n-1}+F_{n-2})x^n \\
&= 1+x+x\sum_{n=2}^{\infty}F_{n-1}x^{n-1} \\
&\quad +x^2\sum_{n=2}^{\infty}F_{n-2}x^{n-2} \\
&= 1+xF(x)+x^2F(x),
\end{aligned}
$$

由此

$$F(x)=(1-x-x^2)^{-1}. \tag{1}$$

此即 Fibonacci 数的生成函数． 因 $1-x-x^2$ 的二个根为 $\alpha=(1+\sqrt{5})/2$, $\beta=(1-\sqrt{5})/2$,于是

$$
\begin{aligned}
(1-x-x^2)^{-1} &= (1-\alpha x)^{-1}(1-\beta x)^{-1} \\
&= ((\alpha/1-\alpha x)-(\beta/1-\beta x))/\alpha-\beta \\
&= \sum_{n=0}^{\infty}((\alpha^{n+1}-\beta^{n+1})/\alpha-\beta)x^n.
\end{aligned}
$$

因此

$$F_n=(\alpha^{n+1}-\beta^{n+1})/\alpha-\beta. \tag{2}$$

我们曾在 1.3 节中用二项式系数表出过 F_n ((1.3.8)式)．若从 $\sum F_nx^n=(1-(x+x^2))^{-1}=\sum(x+x^2)^n$ 比较系数还可得出 F_n 的另一种用二项式系数表出的方式：

$$F_n=\sum_k\binom{n-k}{k}. \tag{3}$$



由此表示式可以推出 Fibonacci 数的组合学意义如下

命题 1. F_n 等于集合 $\mathscr{N}_{n-1}=\{1,2,\cdots,n-1\}$ 中不含两个相邻元的子集个数。例如，$\mathscr{N}_3=\{1,2,3\}$ 的此种子集有 $\varnothing,\{1\},\{2\},\{3\},\{1,3\}$ 共 $F_4=5$ 个。

证. 以 $f(n,k)$ 表示 $\mathscr{N}_n=\{1,2,\cdots,n\}$ 中不包含相邻元的 k-子集(即有 k 个元的子集)个数。设 $\{i_1,i_2,\cdots,i_k\}$ 为此种 k-子集，其中 $i_1<i_2<\cdots<i_k$，由不相邻性可知 $i_s-i_{s-1}\geqslant 2$，于是若记 $j_s=i_s-s$，则必有 $j_s>j_{s-1}$，反之由 $j_s>j_{s-1}$ 也可推出 $i_s-i_{s-1}\geqslant 2$。因此此种 k-子集 $\{i_1,i_2,\cdots,i_k\}$ 与集合 $\{j_1,\cdots,j_k\}$ 一一对应。但 $j_1=i_1-1\geqslant 0$，$j_k=i_k-k\leqslant n-k$，故 $\{j_1,\cdots,j_k\}$ 为 $\{0,1,\cdots,n-k\}$ 的一个 k-子集，故有 $\binom{n-k+1}{k}$ 种取法，由此可见 $f(n,k)=\binom{n-k+1}{k}$. 因此 $\sum\limits_k\binom{n-k+1}{k}$ 即表示 $\mathscr{N}_n$ 中所有不包含相邻元的子集个数。

注. 与数 $f(n,k)$ 相关的另有一组数 $f^*(n,k)$，定义为 $\{1,2,\cdots,n\}$ 的不包含 $(1,2,\cdots,n,1)$ 中相邻二元的 k-子集个数。今证

$$f^*(n,k)=\frac{n}{n-k}\binom{n-k}{k}. \tag{4}$$

实际上若将满足所述条件的 k-子集分成两类，第一类不包含数 n，第二类包含数 n，第一类 k-子集便在 $\{1,2,\cdots,n-1\}$ 中选取，计有 $f(n-1,k)$ 种取法；而第二类 k-子集必不包含 1 与 $n-1$，故除去数 n 外，余下 $k-1$ 个元须在 $\{2,3,\cdots,n-2\}$ 中选取，计有 $f(n-3,k-1)$ 种取法。因此

$$f^*(n,k)=f(n-3,k-1)+f(n-1,k)$$



$$=\binom{n-k-1}{k-1}+\binom{n-k}{k}=\frac{n}{n-k}\binom{n-k}{k}.$$

Fibonacci 数有很多有趣的性质，下面我们利用生成函数(1)导出其中的一部分．考察

$$\sum_{n=0}^{\infty} F_{n+m}x^{n+m}=F(x)-(1+x+\cdots+F_{m-1}x^{m-1})$$
$$=(1-(1-x-x^2)(1+x+\cdots$$
$$+F_{m-1}x^{m-1}))F(x)$$
$$=(F_m x^m+F_{m-1}x^{m+1})F(x),$$

比较两边 x^{n+m} 前系数便得

$$F_{n+m}=F_mF_n+F_{m-1}F_{n-1}. \tag{5}$$

由此式出发，利用 Euclid 算法可以证得 Fibonacci 数的一个重要性质

$$\gcd(F_m,F_n)=F_{\gcd(m,n)}, \tag{6}$$

其中 $\gcd(a,b)$ 表示 a 与 b 的最大公约数．

又如我们注意到对任一级数 $\sum a_nx^n$，有$(1-x)^{-1}\sum a_nx^n=\sum_n\left(\sum_{i=0}^{n}a_i\right)x^n$ 成立，于是从

$$1=F(x)(1-x-x^2)=F(x)(2-x-x^2)-F(x),$$

得

$$F(x)=F(x)(2-x-x^2)-1$$
$$=F(x)(2+x)(1-x)-1,$$
$$(1-x)^{-1}F(x)=F(x)(2+x)-(1-x)^{-1}.$$

比较两边 x^n 之系数即得

$$F_0+F_1+F_2+\cdots+F_n=F_{n+2}-1. \tag{7}$$

Fibonacci 数列是应用中最重要的数列之一． 在历史上，Lamé 首先应用 Fibonacci 数研究了 Euclid 算法的有效性．其后 Lucas 曾利用 Fibonacci 数证明了 $2^{127}-1$ 为素数． 在近



代，Fibonacci 数则出现于各种搜索问题的算法中（见 Knuth [98] V.3）．我国近年来由华罗庚教授倡导的“优选法”中，基本常数 0.618 即来源于 Fibonacci 数列：

$$\lim_{n\to\infty} F_{n-1}/F_n = 1/\alpha = 0.618033\cdots. \tag{8}$$

在生产实践中，我们常需通过若干次试验定出某个单因素函数 $f(x)$ 的最佳点，例如最优的配方比例，最合适的反应温度等等．当 $f(x)$ 为区间 $[c_1, c_2]$ 上的状如图 1 的“单峰”函数（亦即区间中只有一个相

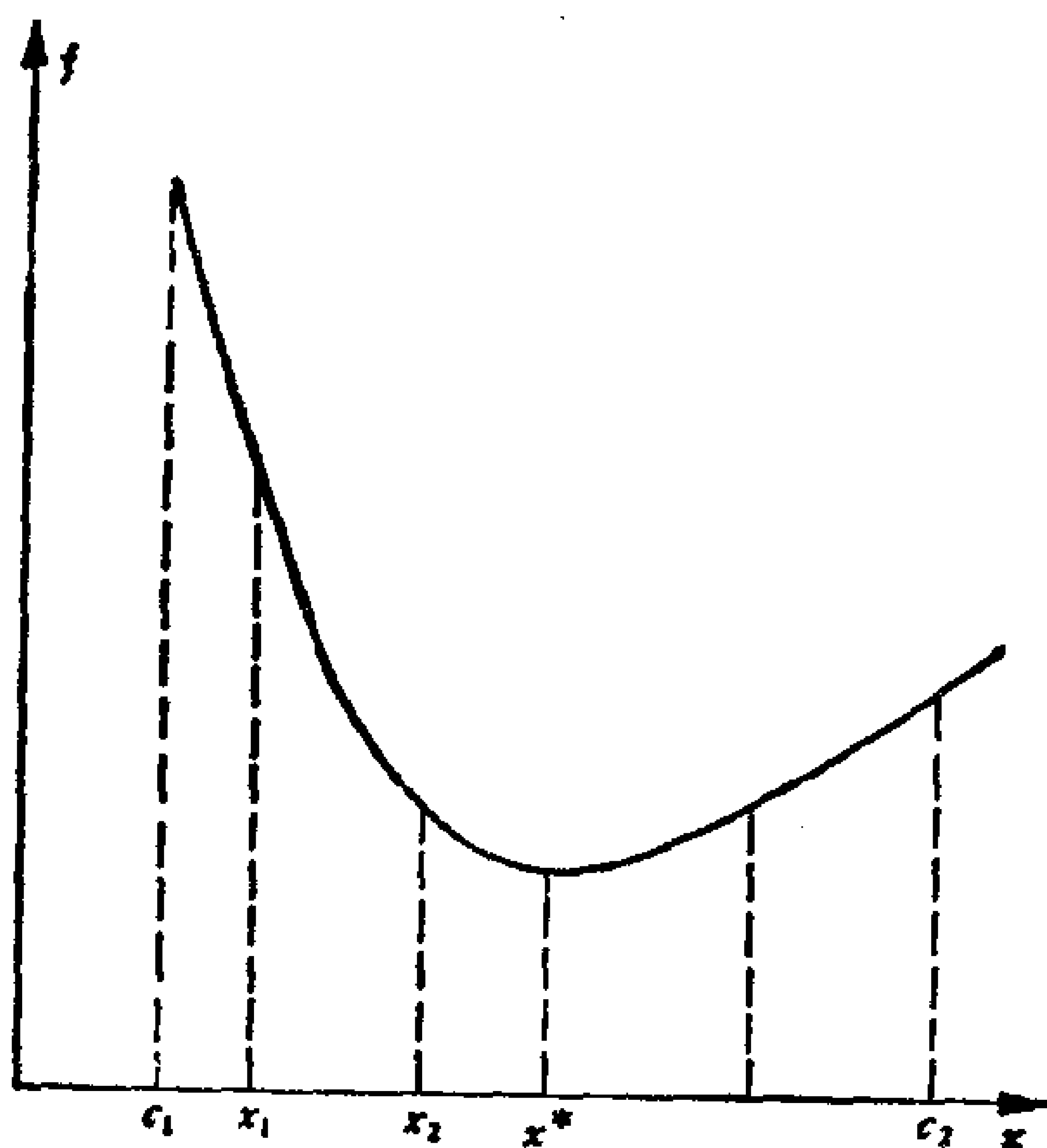


图 1． 单峰函数

对极值点）时，我们可根据各次试验点的取值来判断最佳点 x^* 的位置．例如当 x^* 为 $f(x)$ 的最小值点时，若 $f(x_2)<f(x_1)$，则 x^* 必在 $[x_1, c_2]$ 内，因而下一步的试验点就可在 $[x_1, c_2]$ 中选取．此时 $[x_1, c_2]$ 就称为“留下的范围”，而留在此区间中的已作过试验的点 x_2 即称为“留下试验点”．

今问：当试验次数 N 确定后，应如何安排这 N 个试验点，使最优试验点（即 N 个点中 f 取值最佳的一点）与最佳点 x^* 的距离尽可能地近？

对此，在“优选法”理论中蒲吉[12]证明了：



定理 A. 当试验次数 N 确定后，N 个试验点的最优选取策略可使最优试验点与最佳点的位置之距离不超过 d/F_{N+1}，其中 $d = c_2 - c_1$ 为试验开始时区间的长度。为此，头两个试验点可取为距两端各为 $(F_N/F_{N+1})d$ 的位置对称的两点，然后每次比较前后两次试验点上的值，决定留下范围，并按与留下试验点为对称的原则选取下一试验点.

上述试验点的选取方式称为“分数法”. 在应用中试验次数 n 由问题所需求的精度确定. 例如要求精度为试验范围长度的千分之一时，则因 $F_{15} = 987$，$F_{16} = 1597$，知共需做 15 次. 这较之用等分试验区间来取试验点的“均分法”所需次数少得多.

当 n 充分大时，由 (2) 式可见，前后两个 Fibonacci 数之比趋于常值 0.618033…，因此头两个试验点可近似取为试验范围的 0.382 和 0.618 处，以后各个试验点仍按前述的对称方式选取. 这种方法称为“0.618 法”，又称“黄金分割法”. 它的优点是不用记住各个 F_n，而且华罗庚教授指出：采用 0.618 法至多比分数法多做一次试验. 由于 0.618 法简单易行，故目前在国内很多生产部门中已广泛推广使用，并收到了很好的成效.

2.2. 生成函数的基本方法

在组合计数问题中最常应用下面两种形式的生成函数：

(i) 寻常生成函数

$$A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots. \qquad (1)$$

(ii) 指数生成函数

$$A(x) = a_0 + a_1x + a_2\frac{x^2}{2!} + \cdots + a_n\frac{x^n}{n!} + \cdots. \qquad (2)$$

式中变量 x 一般取自实数或复数域. 一般我们希望级数(1)与(2)有一确定的收敛半径. 不过在应用中通常我们对级数的收敛性并不特别关注，也不去过分计较施于无穷和式中的各种运算如乘法，微分等的合法性. 这是因为一方面我们确实



可以建立一套关于形式幂级数的严谨的数学理论(见 Doubilet *et al.* [57], Niven [119]),此时变量 x 只是一种形式变元,对此种级数可按通常方式定义其加法、乘法、形式微分等运算,从而构成一种代数体系,其中不涉及收敛性等度量性质;另一方面,我们可以把生成函数方法看作是一种推导结果的有效工具,待得出结果后,再来严格地证明(比如用数学归纳法)结果本身. 后面这一步通常要容易些. 比如要从一个形式复杂的递推式出发来导出它的解表示式常常比验证某个表示式满足此递推式来得困难. 当然在大多数场合,当变元 x 看作是复数时,由分析学中已知结果,可以确保所得结果的正确性. 因而在下面的讨论中,我们将着重于方法本身的介绍,而不去计较收敛性问题.

生成函数的一般形式是

$$G(x) = a_0g_0(x) + a_1g_1(x) + a_2g_2(x) + \cdots + a_ng_n(x) + \cdots. \qquad (3)$$

为了确保表示方式 $\sum a_ig_i(x)$ 的唯一性,这里应要求诸函数 $g_n(x)$ 线性无关. 上式当 $g_n(x) = x^n$ 及 $x^n/n!$ 时即分别得出(1)与(2). $g_n(x)$ 的其他例子如

(i) $g_n(x) = 1/n^x$ (Dirichlet 生成函数),

$$A(x) = a_1 + a_2/2^x + a_3/3^x + \cdots + a_n/n^x + \cdots. \qquad (4)$$

(ii) $g_n(x) = [x]_n$ (下阶乘生成函数),

$$A(x) = a_0 + a_1x + a_2x(x-1) + \cdots + a_n[x]_n + \cdots. \qquad (5)$$

由生成函数之定义易知若 $A(x)$, $B(x)$ 分别为 $\{a_i\}$ 与 $\{b_i\}$ 的生成函数,则 $C(x) = A(x) + B(x)$ 为 $\{c_i\}$,其中 $c_i = a_i + b_i$ 的生成函数. 对于与积 $C(x) = A(x)B(x)$ 相应的序列 $\{c_i\}$ 则有

(i) 在寻常生成函数 $A(x) = \sum a_ix^i$, $B(x) = \sum b_ix^i$ 的



情形

$$c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0. \qquad (6)$$

特别取 $B(x) = \sum x^n = (1-x)^{-1}$ 可见，若 $\{a_i\}$ 之生成函数为 $A(x)$，则 $\left\{\sum_{i=1}^{n} a_i\right\}$ 之生成函数为 $(1-x)^{-1}A(x)$.

(ii) 在指数生成函数 $A(x)=\sum a_i x^i/i!$，$B(x)=\sum b_i x^i/i!$ 的情形

$$c_n = a_0 b_n + \binom{n}{1} a_1 b_{n-1} + \cdots + \binom{n}{i} a_i b_{n-i} + \cdots + a_n b_0. \qquad (7)$$

此式将在后面反复引用.

(iii) 在 Dirichlet 生成函数 $A(x) = \sum a_i/i^x$，$B(x) = \sum b_i/i^x$ 的情形

$$c_n = \sum_{ij=n} a_i b_j. \qquad (8)$$

寻求生成函数的一般方法是从 a_n 之组合意义入手，或推出它所适合的递推式，由此导出生成函数 $G(x)$ 所满足的方程，从中解出 $G(x)$. 今举数例加以说明.

1. 在二项式定理的证明中，我们注意到 $(1+x)^n = (1+x)(1+x)\cdots(1+x)$，由于每个括号都是 x 的一次式，因此为了形成 x^k，每个括号中的 x 或者不取，或者只取一次. 今若将每个括号 $(1+x)$ 改成 $(1+x+x^2)$，则为了形成 $x^k = x\cdot x\cdots x$，其中的 $x\cdot x$ 既可取自不同的括号，也可取自同一括号 $(1+x+x^2)$ 中的 x^2. 由此可见 $f(x) = (1+x+x^2)^n$ 的展开式中，x^k 前的系数等于 n 个元 $a, b, c, \cdots$ 的 k-组合个数 c_k，其中每个元 a, b, c 等至多重复二次. 换言之 $f(x)$ 为 c_k 的生成函数. 因



$$f(x)=(1+x+x^2)^n=\sum_{k_1+k_2+k_3=n}\binom{n}{k_1,k_2,k_3}x^{k_2}x^{2k_3}$$

$$=\sum_{k=0}^{n}\left(\sum_{\substack{k_2+2k_3=k\\k_1+k_2+k_3=n}}\binom{n}{k_1,k_2,k_3}\right)x^k,$$

因此

$$c_k=\sum_{\substack{k_2+2k_3=k\\k_1+k_2+k_3=n}}\binom{n}{k_1,k_2,k_3}$$

$$=\sum_{s=0}^{[k/2]}\binom{n}{n-k+s,k-2s,s}$$

$$=\sum_{s=0}^{[k/2]}\frac{n!}{(n-k+s)!(k-2s)!s!}.$$

例如当 $n=k=3$ 时共有 $\binom{3}{0,3,0}+\binom{3}{1,1,1}=1+6=7$ 种组合，它们是

$$\{a,a,b\},\ \{a,a,c\},\ \{b,b,a\},\ \{b,b,c\},$$
$$\{c,c,a\},\ \{c,c,b\},\ \{a,b,c\}.$$

用类似的方法讨论可见，n 个元的重复次数不限的 k-组合个数 c_k 的生成函数为 $(1+x+x^2+\cdots)^n=(1-x)^{-n}$，因此 $c_k=(-1)^k\binom{-n}{k}=\binom{n+k-1}{k}$，与命题(1.1.4)一致。

又如对于 n 个元重复次数不限，但每个元至少出现一次的 k 组合个数 c_k，其生成函数为

$$(x+x^2+x^3+\cdots)^n=x^n(1-x)^{-n}$$

$$=x^n\sum\binom{-n}{k}(-1)^kx^k=\sum\binom{n+k-1}{k}x^{n+k}$$

$$=\sum_{k=n}^{\infty}\binom{k-1}{k-n}x^k,$$



因此 $c_k = 0, (k < n)$; $c_k = \binom{k-1}{k-n}, (k \geqslant n)$.

2. 命题 1.

$$\sum_{\substack{i_1+2i_2+\cdots+(m+k)i_{m+k}=m+k \\ i_1+i_2+\cdots+i_{m+k}=m}} \binom{m}{i_1, \cdots, i_{m+k}} = \binom{m+k-1}{k}. \tag{9}$$

证. 我们知道 $\binom{m}{i_1, i_2, \cdots, i_{m+k}}$ 来自 $(x_1 + \cdots + x_{m+k})^m$ 的展开式中 $x_1^{i_1}\cdots x_{m+k}^{i_{m+k}}$ 之系数，而为了形成所求的和式，显然可取 $x_1 = x, x_2 = x^2, x_3 = x^3, \cdots$. 因此我们选用生成函数

$$(x + x^2 + x^3 + \cdots + x^{m+k})^m$$

$$= \sum_p \Bigg(\sum_{\substack{i_1+2i_2+\cdots+(m+k)i_{m+k}=p \\ i_1+i_2+\cdots+i_{m+k}=m}} \binom{m}{i_1, \cdots, i_{m+k}} \Bigg) x^p.$$

故 (9) 式左边等于 $(x + x^2 + \cdots + x^{m+k})^m$ 展开式中 x^{m+k} 的系数，此又显然等于 $(x + x^2 + \cdots + x^{m+k} + x^{m+k+1} + \cdots)^m = x^m(1-x)^{-m}$ 展开式中 x^{m+k} 的系数，从而等于 $\binom{-m}{k} \cdot (-1)^k = \binom{m+k-1}{k}$.

3. 二元树的计数问题. 所谓二元树乃状如图 2 所示的结构. 点 A 称作树的“根点”, G, H, I, J 称作“叶点”，过每一点往上至多有两个分支. 若将根点 A 去掉即得二个子树：左子树 $\{B, D, E, G, H, I\}$ 与右子树 $\{C, F, J\}$，各以 B, C 为根点，于是二元树可归纳定义为：空集或一组有限个顶点，满足：(i) 有一个特定的点称作“根点”；(ii) 去掉这个根点后，余下的顶点组成两支子二元树：左子树与右子树.



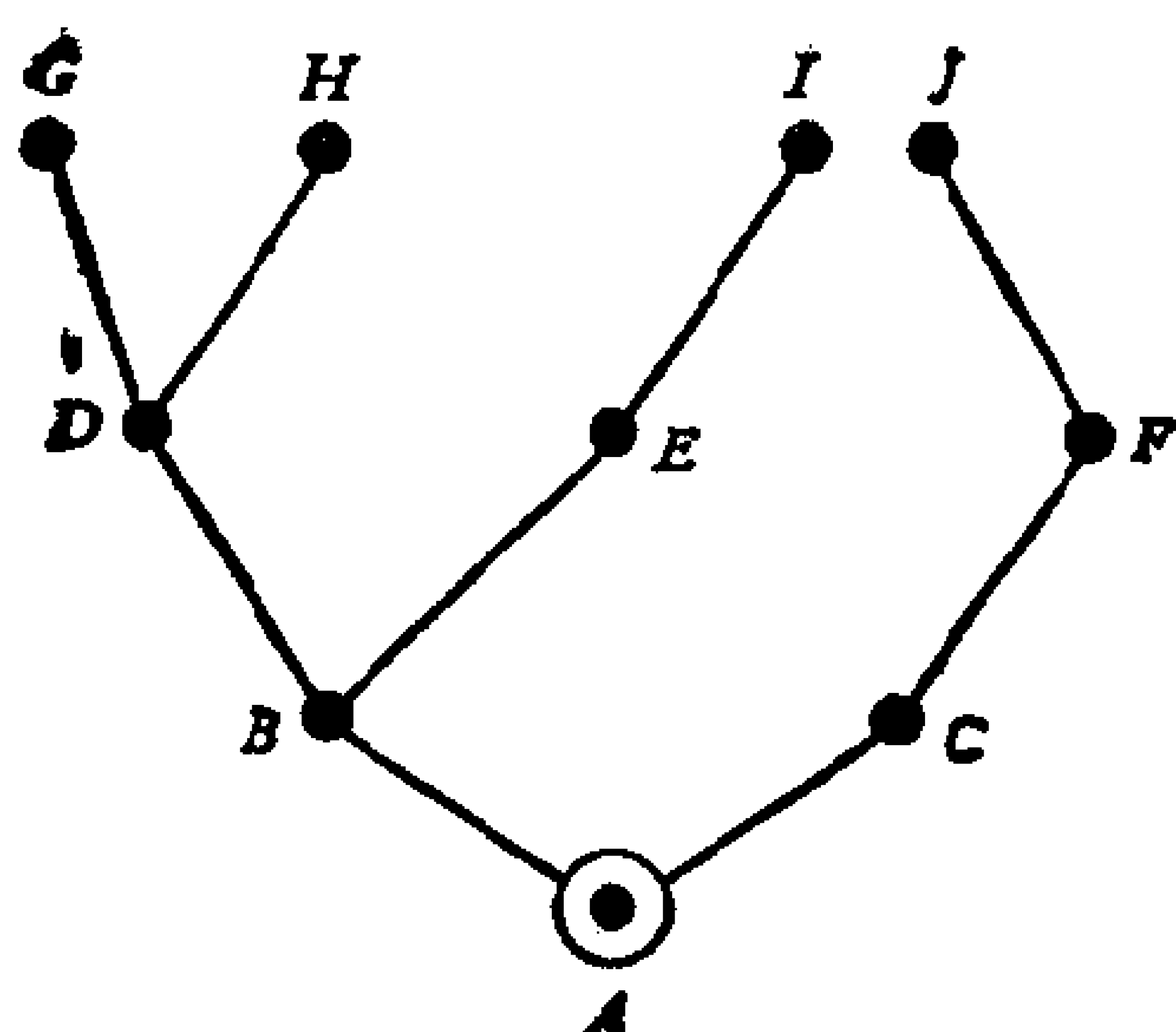


图 2.　二元树

树形结构反映了元间的分支关系，是应用中一类非常重要的结构. 在 Knuth [98] V.1, V.2, V.3 中详细地描述了计算机信息存储的树形结构，并讨论了与之相关的许多算法，从中引出了下面的二元树之计数问题：

"有多少种由 n 个顶点组成的二元树？"

例如，3 个顶点可组成 5 种二元树（图 3).

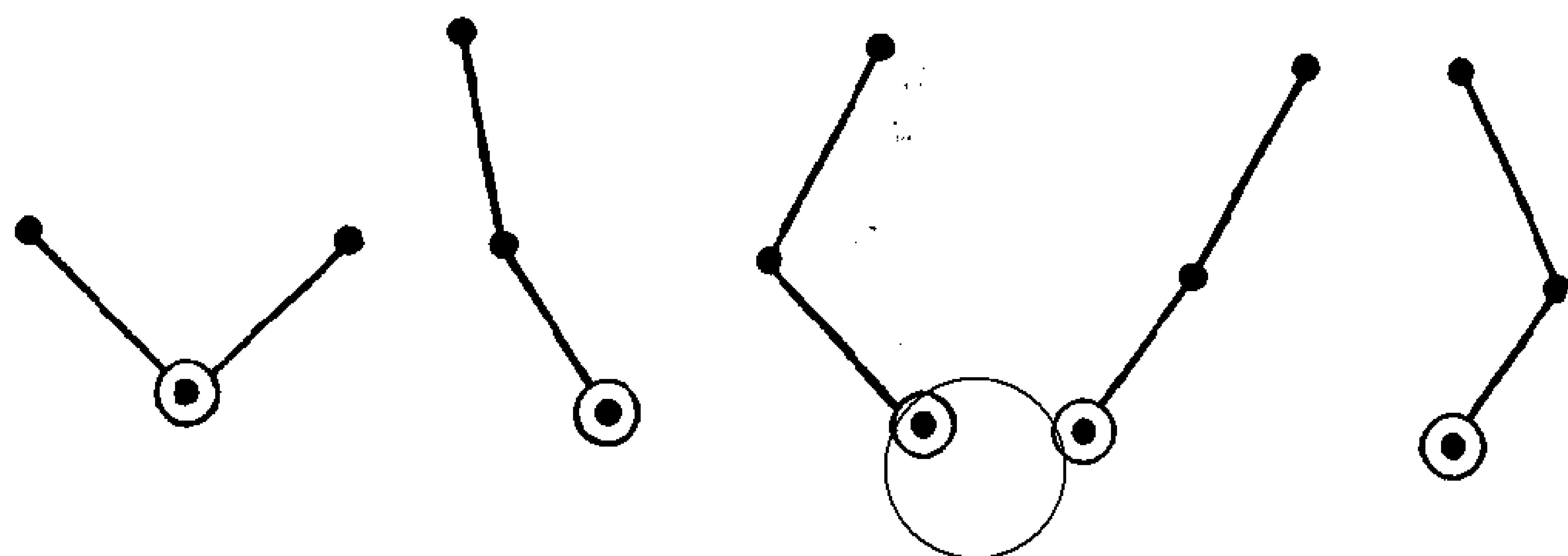


图 3.　三个顶点的二元树

一般设 b_n 为 n 个顶点的不同二元树的个数，则显见 $b_0=1$（空二元树). 在 $n>0$ 的情形，二元树有 1 个根点及 $n-1$ 个非根点，后者可分为二组分别形成左子树与右子树. 设左子树有 k 个点，右子树有 $n-1-k$ 个点，则左子树有 b_k 种取法，右子树有 b_{n-1-k} 种取法. 因此

$$b_n=b_0b_{n-1}+b_1b_{n-2}+\cdots+b_{n-1}b_0 \qquad (n>0).$$

比较上式与(6)式可见其生成函数 $B(x)=b_0+b_1x+b_2x^2+$



· · ·满足方程

$$xB(x)^2 = B(x) - 1,\quad B(0) = 1.$$

解此二次方程,并应用二项式定理即得

$$B(x) = (1 - \sqrt{1-4x})/2x$$

$$= \left(1 - \sum_{n\geq 0} \binom{\frac{1}{2}}{n} (-4x)^n\right) \Big/ 2x$$

$$= \sum_{n\geq 0} \binom{\frac{1}{2}}{n+1} (-1)^n 2^{2n+1} x^n.$$

因此

$$b_n = \binom{\frac{1}{2}}{n+1} (-1)^n 2^{2n+1} = \binom{2n}{n} \Big/ (n+1). \qquad (10)$$

这一数列通称为 Catalan 数,有很多种组合意义.例如 b_n 表示圆周上的 $2n$ 个点可以用 n 条互不相交的弦连结的不同方式个数等等. 关于 b_n 的综述性文件可见 Alter [22].

4. 求不定方程 $x + 2y + 3z = n$ 的非负整数解的个数 A_n. 为此选取生成函数

$$G(x) = ((1-x)(1-x^2)(1-x^3))^{-1}$$

$$= \sum x^i \sum x^{2j} \sum x^{3k} = \sum x^{i+2j+3k} = \sum A_n x^n.$$

将 $G(x)$ 展成部分分式, 记 $\omega = \exp(2\pi i/3)$ 为 1 的 3 次根,于是

$$G(x) = \frac{1}{(1-x)^3(1+x)(1-\omega x)(1-\omega^2 x)}$$

$$= \frac{1}{6(1-x)^3} + \frac{1}{4(1-x)^2} + \frac{17}{72(1-x)}$$



$$+\frac{1}{8(1+x)}+\frac{1}{9(1-\omega x)}+\frac{1}{9(1-\omega^2 x)}$$

$$=\sum_{n=1}^{\infty}\left(\frac{(n+3)^2}{12}-\frac{7}{72}+\frac{(-1)^n}{8}\right.$$

$$\left.+\frac{2}{9}\cos\frac{2n\pi}{3}\right).$$

因此

$$A_n=\frac{(n+3)^2}{12}-\frac{7}{72}+\frac{(-1)^n}{8}+\frac{2}{9}\cos\frac{2n\pi}{3}$$

若用 $\|x\|$ 表示与 x 最接近的整数，则 A_n 可表示成

$$A_n=\left\|\frac{(n+3)^2}{12}\right\|,$$

因此

$$\left|-\frac{7}{72}+\frac{(-1)^n}{8}+\frac{2}{9}\cos\frac{2n\pi}{3}\right|\leqslant\frac{32}{72}<\frac{1}{2}.$$

一般设 $a_1, a_2, \cdots, a_k$ 为 k 个正整数，则不定方程 $a_1x_1+\cdots+a_kx_k=n$ 对任一 n 有非负解的必要条件为 $a_1, a_2, \cdots, a_k$ 互素. 此时若记方程解的个数为 A_n，则仿前，A_n 的生成函数即为

$$G(x)=((1-x^{a_1})(1-x^{a_2})\cdots(1-x^{a_k}))^{-1}.$$

我们将在 4.3 节中由此式出发证明 A_n 的渐近值为 $n^{k-1}/((a_1a_2\cdots a_k)(k-1)!)$.

在涉及到与排列问题有关的生成函数时，我们通常使用指数生成函数. 例如由

$$(1+x)^n=\sum_k [n]_k x^k/k!$$

可见 $(1+x)^n$ 是 $[n]_k$ 的指数生成函数. 在一般情形，若元 a_1 可以重复 $\alpha_1, \alpha_2, \cdots$ 次，a_2 可以重复 $\beta_1, \beta_2, \cdots$ 次，$\cdots$，元 a_n 可以重复 $\lambda_1, \lambda_2, \cdots$ 次，则元 $a_1, a_2, \cdots a_n$ 的此种 k-



排列个数 P_k 之生成函数为

$$\sum_k P_k \frac{xk}{k!} = \left(\frac{x^{\alpha_1}}{\alpha_1!} + \frac{x^{\alpha_2}}{\alpha_2!} + \cdots\right)$$

$$\times \left(\frac{x^{\beta_1}}{\beta_1!} + \frac{x^{\beta_2}}{\beta_2!} + \cdots\right) \cdots \left(\frac{x^{\lambda_1}}{\lambda_1!} + \frac{x^{\lambda_2}}{\lambda_2!} + \cdots\right).$$

实际上,上式右边之积等于

$$\sum_k \left(\sum_{\alpha_{i_1}+\beta_{i_2}+\cdots+\lambda_{i_n}=k} \frac{k!}{\alpha_{i_1}!\beta_{i_2}!\cdots\lambda_{i_n}!} \right) \frac{x^k}{k!}.$$

而由命题(1.2.2), $\frac{k!}{\alpha_{i_1}!\beta_{i_2}!\cdots\lambda_{i_n}!}$ 正是元 a_1 出现恰为 α_{i_1} 次,元 a_2 出现恰为 β_{i_2} 次,…的 k-排列个数,故按所有可能的 $\alpha_{i_1} + \beta_{i_2} + \cdots = k$ 求和即为总的 k-排列个数 P_k。

例如,当重复次数不限时, P_k 的生成函数为

$$\left(1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots\right)^n$$

$$= (e^x)^n = e^{nx} = \sum n^k \frac{x^k}{k!},$$

亦即 n 种元的重复次数不限的 k-排列个数为 n^k, 与命题(1.1.3)一致.

又如重复次数不限,但每个元至少出现一次的 k-排列个数 P_k 的生成函数为

$$\left(x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots\right)^n = (e^x - 1)^n$$

$$= \sum_{j=0}^{n} \binom{n}{j} (-1)^j e^{(n-j)x}$$

$$= \sum_k \left(\sum_{j=0}^{n} (-1)^j \binom{n}{j} (n-j)^k \right) \frac{x^k}{k!},$$

因此



$$P_k = \sum_{j=0}^{n} (-1)^j \binom{n}{j} (n-j)^k. \qquad (11)$$

应用差分算子 $\Delta f(x) = f(x+1) - f(x)$，移位算子 $Ef(x) = f(x+1)$ 及恒等算子 $If(x) = f(x)$，上式之 P_k 可以简洁地写成

$$P_k = \sum_{j=0}^{n} \binom{n}{j} (-1)^j E^{n-j} 0^k = (E - I)^n 0^k = \Delta^n 0^k.$$

在运用指数生成函数时，还可以应用一种记号方法，即所谓 Blissard 演算法则．下面我们以 (7) 式为例说明这一演算法则的基本思想．

定义移位算子 E_a: $E_a a_i = a_{i+1}$, $E_b b_i = b_{i+1}$. 于是任一指数生成函数 $A(x) = \sum a_i \frac{x^i}{i!}$ 便可写成

$$A(x) = \sum a_i \frac{x^i}{i!} = \sum \frac{x^i}{i!} E_a^i a_0 = e^{xE_a} a_0.$$

同样 $B(x) = e^{xE_b} b_0$，于是积

$$\begin{aligned} A(x)B(x) &= e^{xE_a} a_0 e^{xE_b} b_0 = e^{x(E_a+E_b)} a_0 b_0 \\ &= \sum_n x^n (E_a + E_b)^n / n! \, a_0 b_0. \end{aligned}$$

因此若 $A(x)B(x) = \sum c_n x^n / n!$，则

$$\begin{aligned} c_n &= (E_a + E_b)^n a_0 b_0 = \sum \binom{n}{i} E_a^i E_b^{n-i} a_0 b_0 \\ &= \sum \binom{n}{i} a_i b_{n-i}. \end{aligned}$$

此即(7)式．

上述过程可以更简洁地写成

$$A(x) = e^{ax}, \quad a^i \equiv a_i; \quad B(x) = e^{bx}, \quad b^i \equiv b_i$$

$$c_n = (a + b)^n, \quad a^i \equiv a_i, \quad b^i \equiv b_i.$$

后一式表示将 $(a+b)^n$ 按通常方式展开，然后易 a^i 为 a_i,



b^i 为 b_i. 此种演算法则称为 Blissard 演算法则，它可以表述成：

在开始计算时，将下标移成指数，计算完毕后，再将指数下移成下标.

关于 Blissard 演算法则，我们将在下一节结合复合函数的求导法则继续举例解释.

2.3. 复合函数的求导公式

2.3.1. 求导公式之一

在分析学计算中，我们常需计算函数的高阶导数. 例如作 Taylor 展开时，就需计算各阶导数在某点的值. 设 $x = x(t)$, $f(x) = f(x(t))$ 为 t 的复合函数，则由复合函数求导法则，有

$$D_t f = D_x f \cdot D_t x \tag{1}$$

其中 $D_t = d/dt$, $D_x = d/dx$. 反复应用(1)式，并记 $D_x^n f = f_n$, $D_t^n x = x_n$, 可得 $D_t^2 f = f_1 x_2 + f_2 x_1^2$, $D_t^3 f = f_1 x_3 + f_2 x_2 x_1 + 2 f_2 x_1 x_2 + f_3 x_1^3 = f_1 x_3 + 3 x_1 x_2 f_2 + f_3 x_1^3$. 随着 k 的增大, $D_t^n f$ 的表示式越来越繁复，因而需要一种系统的推导法则.

下面的求导公式将 $D_t^n f$ 之计算归结为 $D_t^n x^i$ 之计算.

命题 1.

$$D_t^n f(x) = \sum_{k=0}^{n} \left(\frac{(-1)^k}{k!}\right) D_x^k f(x) \times \sum_{j=0}^{k} (-1)^j \binom{k}{j} x^{k-j} D_t^n x^j. \tag{2}$$

有关此公式的文献见 Gould [73]. 下面我们给出此式的一种启发式推导，它可以帮助我们记住这一看去形式复杂的



公式。

设 $f(x)$ 可展成 Taylor 级数，且可对之逐项微分，则有

$$f(x(t)) = \sum_k D_x^k f(x(s))(x(t)-x(s))^k/k!$$

$$= \sum_k ((-1)^k/k!)D_x^k f(x(s))$$

$$\times \sum_{j=0}^{k}(-1)^j\binom{k}{j}x(s)^{k-j}x^j(t).$$

两边施以算子 D_t^n 得

$$D_t^n f(x(t)) = \sum_{k=0}^{n}((-1)^k/k!)D_x^k f(x(s))$$

$$\times \sum_{j=0}^{k}(-1)^j\binom{k}{j}x(s)^{k-j}D_t^n x^j(t)$$

$$+ \sum_{k>n}(D_x^k f(x(s))/k!)D_t^n(x(t)-x(s))^k.$$

但易见第二个和式当 $t=s$ 时为零，由此令 $s=t$ 即得(2)。

在(2)中取 $f(x)=x^{-1}$，即得

$$D_t^n(1/x) = \sum_{j=0}^{n}(-1)^j\binom{n+1}{j+1}x^{-j-1}D_t^n x^j. \tag{3}$$

今举例说明(2)式在 Taylor 展开中的应用。

例 1. 求 $t/(e^t-1) = \sum_n B_n t^n/n!$. (4)

$$B_n = D_t^n(t/(e^t-1))_{t=0}$$

$$= \sum_{j=0}^{n}(-1)^j\binom{n+1}{j+1}(D_t^n((e^t-1)/t)^j)_{t=0},$$

但

$$(e^t-1)^j = \sum_{k=0}^{j}(-1)^{j-k}\binom{j}{k}e^{kt}$$



$$= \sum_n (t^{n+j}/(n+j)!)$$

$$\times \sum_{k=0}^{j} (-1)^{j-k} \binom{j}{k} k^{n+j}, \tag{5}$$

故

$$D_t^n((e^t-1)/t)_{t=0}^j = (n!/(n+j)!)$$

$$\times \sum_{k=0}^{j} (-1)^{j-k} \binom{j}{k} k^{n+j}.$$

代入即得

$$B_n = \sum_{j=0}^{n} (-1)^j \binom{n+1}{j+1} (n!/(n+j)!)$$

$$\times \sum_{k=0}^{j} (-1)^{j-k} \binom{j}{k} k^{n+j}. \tag{6}$$

数 B_n 称作 **Bernoulli 数**，在分析学中有很多应用。B_n 还可表成另一种形式，为此令 $x(t) = e^t - 1$，于是

$$t/(e^t-1) = \log(1+(e^t-1))/(e^t-1)$$

$$= \log(1+x)/x = \sum_n (-1)^n x^n/n+1.$$

故对 $f(x) = \log(1+x)/x$ 有 $((-1)^k D_x^k f/k!)_{x=0} = (k+1)^{-1}$，由此应用(2)式即得

$$D_t^n(t/(e^t-1))_{t=0} = \sum_{k=0}^{n} ((-1)^k/(k+1))$$

$$\times (D_t^n(e^t-1)^k)_{t=0}.$$

由(5)式可见

$$B_n = \sum_{k=0}^{n} ((-1)^k/(k+1))$$

$$\times \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} j^n. \tag{7}$$



例2. $\exp(e^t - 1) = \sum_n Y_n t^n / n!$. (8)

取 $x = e^t - 1$, 则 $f(x) = e^x$, $x(0) = 0$. 由(5)式

$$(D_t^n x^j)_{t=0} = \sum_{i=0}^{j} \binom{j}{i} (-1)^{j-i} i^n,$$

故

$$\begin{aligned} Y_n &= (D_t^n e^x)_{t=0} \\ &= \sum_{k=0}^{n} ((-1)^k / k!) \sum_{j=0}^{k} (-1)^j \binom{k}{j} x^{k-j} \\ &\quad \times \left(\sum_{i=0}^{j} \binom{j}{i} (-1)^{j-i} i^n \right) \Bigg|_{x=0}, \end{aligned}$$

即

$$Y_n = \sum_{k=0}^{n} (1/k!) \sum_{i=0}^{k} \binom{k}{i} (-1)^{k-i} i^n. \tag{9}$$

数 Y_n 称作 **Bell 数**. Y_n 与 B_n 也可用**第二类 Stirling 数** $S(n, k)$ 表出，后者定义为

$$(e^t - 1)^k / k! = \sum_n S(n, k) t^n / n!. \tag{10}$$

由(5)式可见

$$\begin{aligned} S(n, k) &= (D_t^n (e^t - 1)^k / k!)_{t=0} \\ &= \left(\frac{1}{k!} \right) \sum_{i=0}^{k} \binom{k}{i} (-1)^{k-i} i^n. \end{aligned} \tag{11}$$

比较(2.2.11)式可见

$$S(n, k) = (\Delta^k 0^n) / k!.$$

比较(9)与(11)式可见

$$Y_n = \sum_{k=0}^{n} S(n, k). \tag{12}$$



因当 $n>0$ 时，$S(n, 0)=0$，故此时 $Y_n=\sum_{k=1}^{n} S(n, k)$，$(n>0)$.

又比较(11)与(7)式可见

$$B_n=\sum_{k=0}^{n}((-1)^k k!/k+1) S(n, k). \tag{13}$$

Bell 数 Y_n 还可表示成

$$Y_n=(1/e) \sum_k k^n/k!, \tag{14}$$

因此

$$\exp(e^x)=\sum_k e^{kx}/k!=\sum_k (1/k!) \sum_n k^n x^n/n!$$

$$=\sum_n (x^n/n!) \sum_{k=0} k^n/k!.$$

2.3.2. 求导公式之二及其推广

本节所介绍的复合函数求导公式将最终用 $D_x^k f(x)$ 及 $D_t^j x(t)$ 来表出 $D_t^n f(x)$.

由归纳法易见

$$D_t^n f(x)=\sum_{k=1}^{n} f_k A_{n,k}(x_1, x_2, \cdots, x_n).$$

其中如前 $f_k=D_x^k f$, $x_j=D_t^j x$, $A_{n,k}$ 为变元 $x_1, x_2, \cdots, x_n$ 之多项式，它与 $f(x)$ 的选取无关．为了定出 $A_{n,k}$ 的表示式，我们选取特殊的 $f(x)=e^{ax}$，此时

$$f_k=a^k e^{ax},$$

$$e^{-ax} D_t^n e^{ax}=\sum_k A_{n,k}(x_1, \cdots, x_n) a^k.$$

将此式记作 $A_n(a; x_1, \cdots, x_n)$ 并简记为 $A_n(a)$,



$$A_n(a) = A_n(a;x_1,\cdots,x_n) = \sum_k A_{n,k}(x_1,\cdots,x_n)a^k,$$

则由 Blissard 演算法则即见

$$D_t^n f(x) = A_n(f;x_1,\cdots,x_n).$$

故问题归为求出 $A_n(a) = e^{-ax}D_t^n e^{ax}$. 由积的求导的 Leibniz 公式

$$\begin{aligned} A_{n+1}(a) &= e^{-ax}D^n(De^{ax}) = e^{-ax}aD^n(e^{ax}x_1) \\ &= a\sum_{k=0}^{n}\binom{n}{k}(e^{-ax}D^{n-k}e^{ax})D^k x_1 \\ &= a\sum_{k=0}^{n}\binom{n}{k}A_{n-k}(a)x_{k+1}. \end{aligned} \tag{15}$$

记 $A_n(a)$ 之指数生成函数为 $E(u)$, ax_{k+1} 之指数生成函数为 $F(u)$,

$$E(u) = e^{uA(a)},\ A^n \equiv A_n;\ F(u) = axe^{xu},\ x^n \equiv x_n.$$

比较(15)与指数生成函数之乘法公式(2.2.7), 可见 $A_{n+1}(a)$ 的生成函数为 $E(u)\cdot axe^{xu}$, 故

$$dE(u)/du = \sum_n A_{n+1}(a)u^n/n! = E(u)axe^{xu}.$$

积分之,注意到 $E(0)=1$, 即得

$$E(u) = \exp(a(e^{xu}-1)). \tag{16}$$

此处展开 e^{xu} 时, $x^k \equiv x_k$. 将上式展开,比较 $E(u) = \sum_n A_n(a)u^n/n!$, 可见

$$A_n(a) = \sum \frac{n!\,a^k}{k_1!k_2!\cdots k_n!}\left(\frac{x_1}{1!}\right)^{k_1}\cdots\left(\frac{x_n}{n!}\right)^{k_n}. \tag{17}$$

其中和式遍及 $k_1+2k_2+\cdots+nk_n=n$ 的所有非负整数解 $(k_1,\cdots,k_n)$, 而 $k=\sum_i k_i$. 由此推出

命题 2 (di Bruno).



$$D_t^n f = \sum \frac{n! D_x^k f}{k_1! k_2! \cdots k_n!} \times \left(\frac{D_t x}{1!}\right)^{k_1} \left(\frac{D_t^2 x}{2!}\right)^{k_2} \cdots \left(\frac{D_t^n x}{n!}\right)^{k_n}. \qquad (18)$$

其中和式遍及 $k_1 + 2k_2 + \cdots + nk_n = n$ 的所有解 k_i，而 $k = \sum_i k_i$.

多项式 $A_n(1)$ 一般称作 **Bell 多项式**，记作 $Y_n(x_1, x_2, \cdots, x_n)$，

$$Y_n(x_1, \cdots, x_n) = e^{-x} D_t^n e^x, \quad x^k \equiv x_k. \qquad (19)$$

于是它的指数生成函数为

$$Y(u, x) = \sum Y_n(x_1, \cdots, x_n) u^n / n! = \sum A_n(1) u^n / n! = \exp(e^{xu} - 1). \qquad (20)$$

其中 e^{xu} 展开时，$x^k \equiv x_k$. 比较上式与(8)式可见 Bell 数与 Bell 多项式间的关系式

$$Y_n = Y_n(1, 1, \cdots, 1) = \sum n! / (k_1! \cdots k_n! (1!)^{k_1} \cdots (n!)^{k_n}). \qquad (21)$$

其中和式遍及范围与(18)同.

运用行列式之求导公式，(18)式可以写成十分简洁的形式(见 Comtet [51])：

命题 3.

$$D_t^n f = \begin{vmatrix} x_1 D & -1 & 0 & 0 \cdots\cdots \\ x_2 D & x_1 D & -1 & 0 \cdots\cdots \\ x_3 D & 2x_2 D & x_1 D & -1 \cdots\cdots \\ x_4 D & 3x_3 D & 3x_2 D & x_1 D \cdots\cdots \\ \cdots & \cdots & \cdots & \cdots\cdots \end{vmatrix} f. \qquad (22)$$

其中 $D = d/dx$，$x_i = (d/dt)^i x$，行列式中每一行的系数为二项式系数，最后跟以-1.



作为(18)式的应用例子，我们取$x=1/t$，此时$x_i=D_t^i(1/t)=(-1)^i i!\,t^{-i-1}$，故

$$(d/dt)^n F(1/t)=\sum_{\substack{k_1+2k_2+\cdots+nk_n=n\\ k_1+k_2+\cdots+k_n=k}}\frac{n!}{k_1!k_2!\cdots k_n!}\times F^{(k)}\left(\frac{1}{t}\right)(-1)^n t^{-n-k}$$

$$=\sum_{k=1}^{n}\frac{n!}{k!}(-1)^n F^{(k)}\left(\frac{1}{t}\right)t^{-n-k}\times\sum_{\substack{k_1+2k_2+\cdots=n\\ k_1+k_2+\cdots=k}}\binom{k}{k_1,\cdots,k_n}$$

$$=\sum_{k=1}^{n}\frac{n!}{(n-k)!}(-1)^n F^{(n-k)}\left(\frac{1}{t}\right)t^{-2n+k}\times\sum_{\substack{k_1+2k_2+\cdots=n\\ k_1+k_2+\cdots=n-k}}\binom{n-k}{k_1,\cdots,k_n}.$$

应用(2.2.9)式知最后一和式等于$\binom{n-1}{k}$，故有

命题 4.

$$(-1)^n\frac{d^n}{dt^n}F\left(\frac{1}{t}\right)=\sum_{k=1}^{n}\frac{(n-1)(n-2)\cdots(n-k)}{x^{2n-k}}\times\binom{n}{k}F^{(n-k)}\left(\frac{1}{t}\right). \tag{23}$$

命题 2 给出了 $f(x(t))$ 的复合函数求导公式，在应用中有时会遇到求更一般的形如



$$f(x_0, x_1, x_2, \cdots, x_n),$$

$$x_i \equiv \frac{d^i x(t)}{dt^i} \qquad (i = 0, 1, 2\cdots)$$

的复合函数求导公式．对此

$$f_t = f_x x_t + f_{x_1}(x_1)_t + \cdots + f_{x_n}(x_n)_t.$$

但 $(x_i)_t = x_{i+1}$，故写成算子形式即

$$D_t = \sum_{j=0}^{n} x_{j+1}\partial_j, \quad \partial_j \equiv \frac{\partial}{\partial x_j}. \tag{24}$$

由此进而计算

$$D_t^2 = \left(\sum_i x_{i+1}\partial_i\right)\left(\sum_j x_{j+1}\partial_j\right)$$

$$= \sum_i x_{i+1}(\partial_i x_{j+1})\partial_j + \sum_{ij} x_{i+1}x_{j+1}\partial_i\partial_j.$$

但 $\partial_i x_{j+1} = \delta_{i,j+1}$ ($\delta_{i,j}$ 表示 Kronecker 符号)，故

$$D_t^2 = \sum_i x_{i+2}\partial_i + \sum_{i,j} x_{i+1}x_{j+1}\partial_i\partial_j. \tag{25}$$

一般我们有

命题 5.

$$D_t^m = \sum_{r=1}^{m} \sum_{i_1,\cdots,i_r=0}^{n} \sum_{\substack{s_1+\cdots+s_r=m \\ s_1,\cdots,s_r>0}} \binom{m}{s_1, s_2, \cdots, s_r}$$

$$\times \frac{x_{i_1+s_1}\cdots x_{i_r+s_r}}{j_1!\,j_2!\cdots j_n!}\partial_{i_1}\partial_{i_2}\cdots\partial_{i_r}. \tag{26}$$

其中 j_k 表示 $(s_1, s_2, \cdots, s_r)$ 中等于 k 的个数．此式当 $n = 0$ 时即化作 di Bruno 公式(18)．

例 1. $m = 3$．$3 = 3 = 1 + 2 = 1 + 1 + 1$，故各项系数分别为

$$\binom{3}{3} = 1, \quad \binom{3}{1,2} = 3, \quad \binom{3}{1,1,1}\frac{1}{3!} = 1,$$



故

$$D_t^3 = \sum x_{i+3}\partial_i + 3\sum x_{i+1}x_{j+2}\partial_i\partial_j + \sum x_{i+1}x_{j+1}x_{k+1}\partial_i\partial_j\partial_k. \qquad (27)$$

$m=4$. $4=4=1+3=2+2=1+1+2=1+1+1+1$，故各项系数分别为

$$\binom{4}{4}=1,\ \binom{4}{1,3}=4,\ \binom{4}{2,2}\frac{1}{2!}=3,$$

$$\binom{4}{1,1,2}\frac{1}{2!}=6,\ \binom{4}{1,1,1,1}\frac{1}{4!}=1,$$

故

$$D_t^4 = \sum x_{i+4}\partial_i + 4\sum x_{i+1}x_{j+3}\partial_i\partial_j + 3\sum x_{i+2}x_{j+2}\partial_i\partial_j + 6\sum x_{i+1}x_{j+1}x_{k+2}\partial_i\partial_j\partial_k + \sum x_{i+1}x_{j+1}x_{k+1}x_{l+1}\partial_i\partial_j\partial_k\partial_l. \qquad (28)$$

公式(26)可由 $D^{m+1}=DD^m$ 出发，对 m 使用归纳法加以证明，证明从略.

2.4. 集合的分划，Stirling 数与 Bell 数

如所周知，对于微分算子 $D=d/dx$ 有 $Dx^n=nx^{n-1}$. 与之相应，对差分算子 $\Delta f(x)=f(x+1)-f(x)$，有

$$\Delta[x]_n = n[x]_{n-1}. \qquad (1)$$

实际上，$\Delta[x]_n=[x+1]_n-[x]_n=(x+1)[x]_{n-1}-[x]_{n-1}\times(x-n+1)=n[x]_{n-1}$. 由此可见 $[x]_n$ 在有限差计算中的地位相当于幂函数 x^n 在分析学中的作用. 例如与 Taylor 公式

$$f(x)=\sum a_n x^n,\ a_n=(D^n f(x)/n!)_{x=0}$$

相应，有



$$f(x)=\sum a_n[x]_n,\quad a_n=(\Delta^n f(x)/n!)_{x=0}. \tag{2}$$

既然 x^n 与 $[x]_n$ 都是首项系数为 1 的 n 次多项式，故它们必能互相表出，而沟通这两类重要函数的桥梁即为 Stirling 数。

定义 1. $[x]_n=\sum_{k=0}^{n}s(n,k)x^k,$

$$x^n=\sum_{k=0}^{n}S(n,k)[x]_k. \tag{3}$$

$s(n,k)$称为第一类 Stirling 数，$S(n,k)$ 称为第二类 Stirling 数。此外，约记

$$[t]_0=t^0=s(0,0)=S(0,0)=1,$$
$$s(n,k)=S(n,k)=0\ (n<k).$$

比较(2)与(3)可见

$$S(n,k)=(\Delta^k x^n/k!)_{x=0}.$$

这与(2.3.11)式一致。

下面的命题汇集了 $s(n,k)$，$S(n,k)$ 的一些最基本的关系式。

命题 1. (i) $s(n+1,k)=s(n,k-1)-ns(n,k),$

$S(n+1,k)=S(n,k-1)+kS(n,k).$

(ii) $s(n+1,k)=\sum_{j=0}^{n}(-1)^j[n]_j s(n-j,k-1),$

$$S(n+1,k)=\sum_{j=0}^{n}\binom{n}{j}S(n-j,k-1). \tag{4}$$

(iii) $\sum_n s(n,k)x^n/n!=(\log(1+x))^k/k!$ (记作$s_k(x)$)，

$\sum_n S(n,k)x^n/n!=(e^x-1)^k/k!$ (记作 $S_k(x)$)。



(iv) $\sum_k S(n,k)s(k,m) = \sum_k s(n,k)S(k,m) = \delta_{n,m}$.

证. (i) 中两式可分别从简单的关系式

$$[x]_{n+1} = [x]_n(x-n),\ x[x]_k = [x]_{k+1} + k[x]_k$$

推出.

(iii) 中第二式即(2.3.10)式. 为证第一式,注意到

$$(ds_k(x)/dx) = \sum_n s(n+1,k)x^n/n!$$
$$= \sum_n s(n,k-1)x^n/n!$$
$$- x\sum_n s(n,k)x^{n-1}/(n-1)!$$
$$= s_{k-1}(x) - x(ds_k(x)/dx),$$

亦即

$$(1+x)(ds_k(x)/dx) = s_{k-1}(x). \tag{5}$$

由此,注意到 $s_k(0) = 1$, $s_0(x) = 1$, 即得

$$s_1(x) = \int_0^x (s_0(t)/(1+t))dt$$
$$= \int_0^x dt/(1+t) = \log(1+x),$$
$$s_2(x) = \int_0^x (s_1(t)/(1+t))dt$$
$$= \int_0^x (\log(1+t)/(1+t))dt$$
$$= (\log(1+x))^2/2!,$$
$$\cdots\cdots\cdots\cdots,$$
$$s_k(x) = \int_0^x (s_{k-1}(t)/(1+t))dt$$
$$= (\log(1+x))^k/k!.$$

为证 (ii) 中第一式,注意到由(5)式得



$$(ds_k(x)/dx) = s_{k-1}(x)(1+x)^{-1},$$

而 $(1+x)^{-1}$ 乃 $(-1)^n/n!$ 的指数生成函数，故由乘法公式(2.2.7)即得证.

(ii) 中第二式之推导相仿.

(iv) 式可从 $x^n = \sum_k S(n,k)[x]_k = \sum_k \sum_m S(n,k) \times s(k,m)x^m$ 及 $[x]_n = \sum_{m,k} s(n,k)S(k,m)[x]_m$ 得出.

命题 2. (i) $[x]^n = \sum_k |s(n,k)|x^k$.

(ii) 对固定的 n (或 k), $s(n,k)$ 随 k (或 n) 的变化而交叉变号.

证. $(-1)^n[x]^n = [-x]_n = \sum_k s(n,k)(-1)^k x^k$, 故

$$[x]^n = \sum_k s(n,k)(-1)^{n+k}x^k.$$

但 $[x]^n = x(x+1)\cdots(x+n-1)$, 其展开式系数均取正值，故 $s(n,k)(-1)^{n+k} > 0$, 即所欲证.

由此命题可以推出

命题 3. $s(n,k) = (-1)^{n+k} \sum_{0<i_1<i_2<\cdots<i_{n-k}<n} i_1 i_2 \cdots i_{n-k}$.

如 $s(5,3) = (-1)^{5+3}(1\times 2 + 1\times 3 + 1\times 4 + 2\times 3 + 2\times 4 + 3\times 4) = 35$.

命题 4. (i) $S(n,k)$ 的寻常生成函数为

$$G_k(x) = \sum_n S(n,k)x^n$$
$$= x^k/((1-x)(1-2x)\cdots(1-kx)). \qquad (6)$$

(ii) $$S(n,k) = \sum_{c_1+c_2+\cdots+c_k=n-k} 1^{c_1}2^{c_2}\cdots k^{c_k}. \qquad (7)$$



证． 由命题1易见 $(1-kx)G_k(x)=xG_{k-1}(x)$．由此即可推出(6)式．又由此式

$$G_k(x)/x^k=\prod_{j=1}^{k}(1-jx)^{-1}=\prod_{j=1}^{k}\sum_{c_j} j^{c_j}x^{c_j},$$

即可推出(7)式；

如 $S(5,2)=1^3+1^2\times 2^1+1^1\times 2^2+2^3=15$.

对于 Stirling 数下列诸等式成立，其证可见 Jordan [91].

命题 5. (i) $s(n,k)=\sum_i(-1)^i\binom{n-1+i}{n-k+i}$

$$\times\binom{2n-k}{n-k-i}S(n-k+i,i).$$

(ii) $S(n,k)=\sum_i(-1)^i\binom{n-1+i}{n-k+i}\binom{2n-k}{n-k-i}$

$$\times s(n-k+i,i).$$

命题 6. $s(p,p)=1$, $s(p,1)=(p-1)!\equiv -1\ (\mathrm{mod}\,p)$, $s(p,k)\equiv 0\ (\mathrm{mod}\,p)$, $(k\neq 1,p)$.

由此还可推出

$$[x]_p=x(x-1)\cdots(x-p+1)\equiv x^p-x\ (\mathrm{mod}\,p).$$

命题 7. $\left(x\dfrac{d}{dx}\right)^n=\sum_{k=1}^{n}S(n,k)x^k(d/dx)^k.$

$$x^n(d/dx)^n=\sum_{k=1}^{n}s(n,k)\left(x\frac{d}{dx}\right)^k.$$

此命题给出了算子 $(x\,d/dx)^n$ 与 $(d/dx)^n$ 的一种很有用的转换关系，可用于一类复合函数的求导运算．例如注意到 $(df/dx)=e^x(df/de^x)$，知 $(d/dx)=(y\,d/dy)$，其中 $y=e^x$．因此 $(d/dx)^nF(e^x)=(y\,d/dy)^nF(y)=\sum_{k=1}^{n}S(n,k)y^k\times(d/dy)^kF(y)$．又如



$$(d/dx)^n F(\log x) = x^{-n} \sum_k s(n, k)(x\, d/dx)^k F(\log x)$$

$$= x^{-n} \sum_k s(n, k) F^{(k)}(\log x).$$

由此推出

命题 8. (i) $(d/dx)^n F(\log x) = x^{-n} \sum_{k=1}^{n} s(n, k) F^{(k)}$ $\times (\log x)$.

(ii) $(d/dx)^n F(e^x) = \sum_{k=1}^{n} S(n, k) e^{kx} F^{(k)}(e^x)$.

第二类 Stirling 数 $S(n, k)$ 的组合学意义涉及到集合的分划.

定义 2. 设 $\mathscr{A}_1, \cdots, \mathscr{A}_k$ 为集合 $\mathscr{A}$ 的一组子集. 若 (i) 诸 $\mathscr{A}_i$ 非空; (ii) $\mathscr{A}_i$ 间互不相交, 亦即 $\mathscr{A}_i \cap \mathscr{A}_j = \varnothing$, $(i \neq j)$; (iii) 诸 $\mathscr{A}_i$ 之并为 $\mathscr{A}$: $\bigcup_{i=1}^{k} \mathscr{A}_i = \mathscr{A}$, 则称子集系 $\mathscr{A}_1, \mathscr{A}_2, \cdots, \mathscr{A}_k$ 构成集合 $\mathscr{A}$ 的一个 k-分划.

命题 9. 一个 n 元的集合有 $S(n, k)$ 种 k-分划. 这里构成分划的各子集之间的次序以及子集中各元的次序均不计.

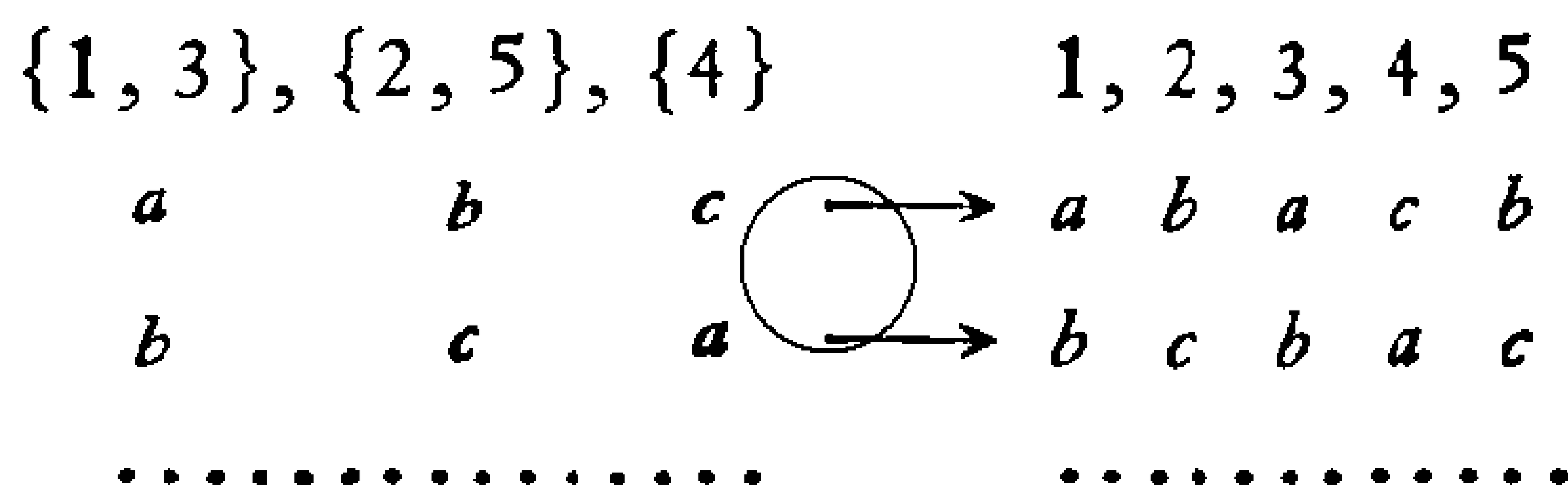
例如当 $n = 4$, $k = 3$ 时, 集合 $\{1, 2, 3, 4\}$ 共有 $S(4, 3) = 6$ 种 3-分划如下:

$$\{\{1, 2\}, \{3\}, \{4\}\}, \quad \{\{1, 3\}, \{2\}, \{4\}\},$$
$$\{\{1, 4\}, \{2\}, \{3\}\}, \quad \{\{2, 3\}, \{1\}, \{4\}\},$$
$$\{\{2, 4\}, \{1\}, \{3\}\}, \quad \{\{3, 4\}, \{1\}, \{2\}\}.$$

证. 对于集合 $\mathscr{A}$ 的每个 k-分划及 k 个字母 $a_1, a_2, \cdots, a_k$ 的任一种 (不带重复的) k-排列, 我们均可作出一个 n-排列, 它由 k 个字母组成, 各字母重复次数不限, 但每个文



字至少出现一次(为叙述方便见，简称此种排列为 $P_{n,k}$ 排列). 例如



k 个字母的两个不同的 k-排列,显然对应两个不同的 $P_{n,k}$ 排列.但 k 个字母有 $k!$ 个不同的排列,因此 $\mathscr{A}$ 的每个 k-分划对应 $k!$ 个不同的 $P_{n,k}$ 排列. 显然不同的分划对应于不同的 $P_{n,k}$ 排列，故若 $\mathscr{A}$ 的 k-分划个数为 $C(n, k)$，则应有 $k!C(n, k)=(P_{n,k}$ 排列的总数$)=\Delta^k 0^n$ (见(2.2.11)式),此即 $C(n, k)=\Delta^k 0^n/k!=S(n, k)$.

由(2.3.12)式，Bell 数 Y_n 满足 $Y_n=\sum\limits_k S(n, k)$,故有

命题 10. 一个 n 元的集合共有 Y_n 种不同的分划.

对于 Bell 数 Y_n 有与(4)式相仿的等式成立:

命题 11. $Y_{n+1}=\sum\limits_{k=0}^{n}\binom{n}{k}Y_k.$ (8)

证. 由 (2.3.8) 式，Y_n 的指数生成函数 $Y(x)=\exp(e^x-1)=\sum\limits_n Y_n x^n/n!$，但 $dY(x)/dx=(\exp(e^x-1))e^x=Y(x)e^x$，注意到 e^x 为 $a_n=1$ 的指数生成函数，故由乘法公式(2.2.7)推知(8)式.

由(8)式可以导出 Y_n 的简便列表算法.

命题 12. $Y_n=\Delta^n Y_1$，此处定义 $\Delta Y_i=Y_{i+1}-Y_i$，从而

$$Y_n=\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}Y_{i+1}. \tag{9}$$



证. $\sum_i (-1)^{n-i} \binom{n}{i} Y_{i+1}$

$$= \sum_{i,j} (-1)^{n-i} \binom{n}{i}\binom{i}{j} Y_j$$

$$= \sum_j \left(\sum_i (-1)^{n-i} \binom{n}{i}\binom{i}{j} \right) Y_j$$

$$= \sum_j \delta_{nj} Y_j = Y_n.$$

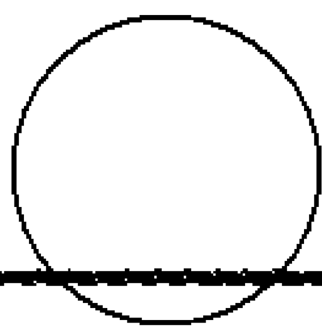


表 1. Y_n 的列表算法

i	1	2	3	4	5
Y_i	1	2	5	15 →	52
ΔY_i	1	3	10 →	37	
$\Delta^2 Y_i$	2	7 →	27		
$\Delta^3 Y_i$	5 →	20			
$\Delta^4 Y_i$	15				
$\Delta^5 Y_i$	(52) ←				

表 2. 第一类 Stirling 数 $s(n, k)$ 表

n \ k	1	2	3	4	5	6	7	8
1	1							
2	−1	1						
3	2	−3	1					
4	−6	11	−6	1				
5	24	−50	35	−10	1			
6	−120	274	−225	85	−15	1		
7	720	−1764	1624	−735	175	−21	1	
8	−5040	13068	−13132	6769	−1960	322	−28	1



此命题给出了逐次计算 Y_n, ΔY_n, $\Delta^2 Y_n \cdots$ 的列表算法，如表 1 所示. 例如已算得 $Y_1=1$, $Y_2=2$, $Y_3=5$, $Y_4=15$ 及 $\Delta Y_1=1$, $\Delta^2 Y_1=2$, $\Delta^3 Y_1=5$ 后，令 $\Delta^4 Y_1=Y_4=15$, $\Delta^3 Y_2=\Delta^4 Y_1+\Delta^3 Y_1=15+5=20$, $\Delta^2 Y_3=\Delta^3 Y_2+\Delta^2 Y_2=20+7=27, \cdots$. 最后 $Y_5=\Delta Y_4+Y_4=37+15=52$, 再令 $\Delta^5 Y_1=52$, 重复上述过程.

表 3. 第二类 Stirling 数 $S(n,k)$ 及 Bell 数 Y_n 表

Y_n	$n \backslash k$	1	2	3	4	5	6	7	8
1	1	1							
2	2	1	1						
5	3	1	3	1					
15	4	1	7	6	1				
52	5	1	15	25	10	1			
203	6	1	31	90	65	15	1		
877	7	1	63	301	350	140	21	1	
4140	8	1	127	966	1701	1050	266	28	1

2.5. Bernoulli 数与多项式，求和公式

2.5.1. Bernoulli 数

Bernoulli 数 B_n 是一类在分析学中应用很多的数. 它的生成函数及表示式为

$$G(x)=\sum B_n x^n/n!=x/(e^x-1),$$

$$B_n=\sum_{k=0}^{n}((-1)^k/(k+1))$$

$$\times \sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}j^n.$$



见(2.3.4)及(2.3.7).

命题1. $\sum_{i=0}^{n}\binom{n}{i}B_i=B_n\ (n>1)$. 用 Blissard 法则可写成

$$(B+1)^n=B^n,\ B^k\equiv B_k\qquad(k>1).$$

证. 由 $x/(e^x-1)=\sum B_nx^n/n!$ 得 $(\sum B_nx^n/n!)e^x=(\sum B_nx^n/n!)+x$, 由指数生成函数的乘法公式 (2.2.7) 即见

$$B_n+\delta_{n,1}=\sum\binom{n}{i}B_i.$$

由命题 1, 及 $B_0=1$ 即可逐次解出 B_i:

$$B_2+2B_1+B_0=B_2,\ B_1=-1/2;$$

$$B_3+3B_2+3B_1+B_0=B_3,\ B_2=1/6;$$

$$B_4+4B_3+6B_2+4B_1+B_0=B_4,\ B_3=0;$$

$$B_5+5B_4+10B_3+10B_2+5B_1+B_0=B_5,\ B_4=-1/30;$$

$$\cdots\quad\cdots\quad\cdots\quad\cdots\cdots\quad\cdots\cdots\cdots\cdots.$$

命题2. $B_{2k+1}=0\qquad(k>0)$.

证. $\sum(-1)^nB_nx^n/n!=(-x)/(e^{-x}-1)=x+(x/(e^x-1))=x+\sum B_nx^n/n!$, 故当 $n>1$ 时, $B_n=(-1)^nB_n$.

命题3. $\zeta(2s)\equiv\sum_{n=0}^{\infty}n^{-2s}=((-1)^{s-1}2^{2s-1}\pi^{2s}/(2s)!)B_{2s}$.

例如 $\zeta(2)=\pi^2/6$, $\zeta(4)=\pi^4/90$, $\zeta(6)=\pi^6/945$, $\zeta(8)=\pi^8/9450$.

证. 我们知道, 若 n 次多项式 $f(x)$ 有 n 个非零根 $a_1,\cdots,a_n$, 则 $f(x)=f(0)\prod_i(1-(x/a_i))$. 注意到 $(\sin\pi x)/\pi x$ 有根 $x=\pm k$, 且当 $x=0$ 时值为 1, 故与此相仿有



$$(\sin \pi x)/\pi x = \prod_{k=1}^{\infty}(1-(x^2/k^2)).$$

此式的严格证明可见 Фихтенгольц [64]．在上式两边取对数可得

$$\log \sin \pi x - \log \pi = \log x + \sum_{k=1}^{\infty}\log(1-(x^2/k^2)).$$

逐项微分得

$$\pi x \cos \pi x/\sin \pi x = 1 - 2\sum_{k=1}^{\infty} x^2/(k^2-x^2)$$

$$= 1 - 2\sum_{k=1}^{\infty}\sum_{s=1}^{\infty} x^{2k}/k^{2s}$$

$$= 1 - 2\sum_{s=1}^{\infty}\left(\sum_{k=1}^{\infty} k^{-2s}\right)x^{2s}. \qquad (1)$$

另一方面应用 $e^{ix} = \cos x + i\sin x \quad (i=\sqrt{-1})$，作代换 $2\pi i x = t$，即得

$$\pi x \cos \pi x/\sin \pi x = (t/2) + (t/(e^t - 1))$$

$$= (t/2) + \sum_{n} B_n t^n/n!$$

$$= 1 + \sum_{s=1}^{\infty} B_{2s}t^{2s}/(2s)!$$

$$= 1 + \sum_{s=1}^{\infty}(B_{2s}(-1)^s 2^{2s}\pi^{2s}/(2s)!)x^{2s}.$$

与(1)式相比较即证得本命题.

由此命题及 $\lim\limits_{s\to\infty}\sum_{n} n^{-2s} = 1$，即得

$$\lim_{s\to\infty}|B_{2s}| \Big/ \left(\frac{(2s)!}{2^{2s-1}\pi^{2s}}\right) = 1. \qquad (2)$$

Bernoulli 数还出现在一些初等函数的 Taylor 展开式中，



例如

命题 4.

(i) $\operatorname{th} x = x - (1/3)x^3 + (2/15)x^5 - (17/315)x^7 + (62/2835)x^9 + \cdots$

$$= \sum_{s=1}^{\infty} B_{2s}2^{2s}(2^{2s}-1)x^{2s-1}/(2s)!.$$

(ii) $\operatorname{tg} x = x + (1/3)x^3 + (2/15)x^5 + (17/315)x^7 + (62/2835)x^9 + \cdots$

$$= \sum_{s=1}^{\infty} B_{2s}(-1)^{s+1}2^{2s}(2^{2s}-1)x^{2s-1}/(2s)!.$$

(iii) $\operatorname{ctg} x = x^{-1} - (1/3)x - (1/45)x^3 - (2/945)x^5 - (1/4725)x^7 - \cdots$

$$= x^{-1} + \sum_{s=1}^{\infty} B_{2s}(-1)^s 2^{2s}x^{2s-1}/(2s)!.$$

(iv) $(\sin x)^{-1} = x^{-1} + (1/6)x + (7/360)x^3 + (31/15120)x^5 + (127/604800)x^7 + \cdots$

$$= x^{-1} + \sum_{s=1}^{\infty} B_{2s}(-1)^{s+1}(2^{2s}-2)x^{2s-1}/(2s)!.$$

证. 由 $\operatorname{th} x = (e^{2x}-1)(e^{2x}+1)^{-1} = 1 - 2(e^{2x}-1)^{-1} + 4(e^{4x}-1)^{-1}$ 即可推出 (i). 再由 $\operatorname{tg} x = -i\operatorname{th}(ix)$ 可推出 (ii), (iii) 与 (iv) 推导方式相仿.

又利用 $\int \operatorname{tg} x dx = -\log\cos x$, $\int \operatorname{ctg} x dx = \log\sin x$, 即可写出 $\log\cos x$ 及 $\log\sin x$ 的展开式等.

2.5.2. Bernoulli 多项式

Bernoulli 多项式 $B_n(y)$ 的生成函数定义为

$$G(x, y) = (xe^{yx})/(e^x - 1)$$



$$= \sum_n B_n(y) x^n / n!. \tag{3}$$

由 $G(x, y) = G(x) \cdot e^{yx}$ 及指数生成函数的乘法公式(2.2.7)可见

命题 5. $B_n(y) = \sum_{i=0}^{n} \binom{n}{i} B_i y^{n-i} = (B + y)^n$, $B^i \equiv B_i$. 特别 $B_n(0) = B_n$.

Bernoulli 多项式的一个重要性质是

命题 6. $\Delta B_n(y) \equiv B_n(y+1) - B_n(y) = n y^{n-1}$.

证. $\sum \Delta B_n(y) x^n / n! = G(x, y+1) - G(x, y)$

$= (x e^{x(y+1)} - x e^{xy})/(e^x - 1) = x e^{xy}$

$= \sum x^{n+1} y^n / n!$.

比较 x^n 前系数即得证.

由此命题便可推知

命题 7. 差分方程 $\Delta F(y) = \sum a_k y^k$ 的一般解为

$$F(y) = \left(\sum_k a_k B_{k+1}(y)/(k+1) \right) + c,$$

其中 c 为与 y 无关的常数.

特别 $\Delta f(x) = x^r$ 的一般解为

$$f(x) = (B_{r+1}(x)/(r+1)) + c. \tag{4}$$

由此推出

命题 8. $\sum_{k=1}^{n} k^r = (B_{r+1}(n+1) - B_{r+1})/(r+1)$

$$= (1/(r+1)) \sum_{i=0}^{r} \binom{r+1}{i} (n+1)^{r+1-i} B_i.$$

证. 记 $C(n, r) = \sum_{k=1}^{n} k^r$, 于是

$$\Delta C(n, r) = C(n+1, r) - C(n, r) = (n+1)^r. \tag{5}$$



比较(5)与(4)可见 $C(n,r)=(B_{r+1}(n+1)+c)/(r+1)$. 令 $n=0$，此时 $C(n,r)=0$，而 $B_{r+1}(1)=(-1)^{r+1}B_{r+1}(0)=(-1)^{r+1}B_{r+1}$，故 $c=(-1)^rB_{r+1}$. 但当 $p\geqslant 1$ 时，$B_{2p+1}=0$，故 $(-1)^rB_{r+1}=-B_{r+1}$. 于是 $C(n,r)=(B_{r+1}(n+1)-B_{r+1})/(r+1)$.

特别

$$\sum_{k=1}^{n} k=n(n+1)/2,$$

$$\sum k^2=n(n+1)(2n+1)/6,$$

$$\sum k^3=n^2(n+1)^2/4,$$

$$\sum k^4=n(n+1)(2n+1)(3n^2+3n-1)/30,$$

$$\sum k^5=n^2(n+1)^2(2n^2+2n-1)/12.$$

命题 9. $y^n=\sum\limits_k\binom{n}{k}(n-k+1)^{-1}B_k(y)$. (6)

证. 设 $y^n=\sum\limits_k c_{n,k}B_k(y)$，则 $\sum\limits_{k=1}^{n}\binom{n}{k-1}y^{k-1}=$

$$\Delta y^n=\sum_k c_{n,k}\Delta B_k(y)=\sum_k c_{n,k}\cdot ky^{k-1}，故 c_{n,k}=$$

$$\binom{n}{k-1}\Big/k=\binom{n}{k}\Big/(n-k+1).$$

命题 10. $B_n(1-y)=(-1)^nB_n(y)$.

证. $\sum\limits_n x^nB_n(1-y)/n!=xe^{x(1-y)}/(e^x-1)$

$$=(-x)e^{y(-x)}/(e^{-x}-1)$$

$$=\sum_n x^n(-1)^nB_n(y)/n!.$$

命题 11. $(d/dyB_n(y))=nB_{n-1}(y)$.



证. $\sum x^n\left(\frac{d}{dy}B_n(y)\right)\Big/n! = (d/dy)(xe^{yx}/(e^x-1))$

$$= x^2e^{yx}/(e^x-1) = \sum x^{n+1}B_n(y)/n!.$$

命题 12. $B_n(my) = m^{n-1}\sum_{i=0}^{m-1} B_n(y+(i/m)).$

证. $\sum_n B_n(my)x^n/n! = xe^{mxy}/(e^x-1)$

$$= (1/m)\sum_{i=0}^{m-1} mxe^{(y+i/m)mx}/(e^{mx}-1)$$

$$= (1/m)\sum_{i=0}^{m-1}\sum_n B_n(y+(i/m))m^nx^n/n!.$$

2.5.3. 求和公式

所谓求和公式,一般系指将和式 $\sum_{k=1}^{n} f(k)$ 转换成更简单或更易于计算的形式. 本节将介绍两种求和公式: Bernoulli 求和公式与 Euler 求和公式. 其中后者在和式转换、渐近计数(见第四章)及积分近似计算(见华罗庚,王元[5])等方面应用更多. 在有限差计算中,还有其他形式的求和公式,可见 Jordan [91].

命题 13 (Bernoulli 求和公式).

$$\sum_{k=1}^{n} f(k) = \binom{n}{1}f(1) + \binom{n}{2}\Delta f(1) + \binom{n}{3}\Delta^2 f(1) + \cdots + \Delta^{n-1}f(1). \tag{7}$$

证. 记 $Ef(x) = f(x+1)$ 为移位算子,于是

$(E-I)(I+E+E^2+\cdots+E^{n-1})$



$$= E^n - I = (\Delta + I)^n - I = \sum_{i=1}^{n} \binom{n}{i} \Delta^i.$$

由此可见

$$I + E + E^2 + \cdots + E^{n-1} = \sum_{i=1}^{n} \binom{n}{i} \Delta^{i-1}.$$

将此式两边算子施于 $f(1)$ 即得所证.

Bernoulli 求和公式一般用于 $f(x)$ 为多项式的场合，此时 f 的高阶差分等于零. 例如对 $f(x) = x^3$，逐次计算 $\Delta^i f(x)$，得

k	1	2	3	4	5
$f(k)$	1	8	27	64	125
$\Delta f(k)$	7	19	37	61	
$\Delta^2 f(k)$	12	18	24		
$\Delta^3 f(k)$	6	6			
$\Delta^4 f(k)$	0				

于是 $f(1) = 1$，$\Delta f(1) = 7$，$\Delta^2 f(1) = 12$，$\Delta^3 f(1) = 6$，应用求和公式即得

$$\sum_{k=1}^{n} k^3 = \binom{n}{1} + 7\binom{n}{2} + 12\binom{n}{3} + 6\binom{n}{4}.$$

命题 14(Euler 求和公式). 设 $f(x)$ 为区间 $[1, n]$ 上的 m 阶连续可微函数，则

$$\sum_{k=1}^{n-1} f(k) = \int_1^n f(x)dx + \left(\sum_{k=1}^{m} B_k(f^{(k-1)}(n) - f^{(k-1)}(1))/k!\right) + R_m. \tag{8}$$

其中 R_m 为余项



$$R_m = ((-1)^{m+1}/m!)\int_1^n B_m(\{x\})f^{(m)}(x)dx.$$

$\{x\}$ 表示 x 的分数部分.

注意到 $B_{2p+1}=0$ $(p>0)$，在(8)式两边加上 $f(n)$，并合并常数项，(8)式还可写成

$$\sum_{k=1}^{n} f(k) = \int_1^n f(x)dx + \left(\sum_{k=1}^{m} B_{2k}f^{(2k-1)}(n)/(2k)!\right) + C + (f(n)/2) + R_{2m}. \tag{9}$$

其中 C 为与 n 无关的常数

$$C = (1/2)f(1) - \sum_{k=1}^{m} B_{2k}f^{(2k-1)}(1)/(2k)!.$$

我们先给出(9)式的一个启发性的推导方式，它可以帮助我们记住此式.

记 $F(n+1)=\sum_{k=0}^{n} f(k)$，于是 $\Delta F(n) = F(n+1) - F(n) = f(n)$. 故问题归结为解差分方程

$$\Delta F(x) = f(x).$$

将此式两边除以算子 Δ，并施以微分算子 $D=(d/dx)$，得

$$DF(x) = D(1/\Delta)f(x).$$

注意到 $Ef(x)=f(x+1)=\sum D^n f(x)/n! = e^D f(x)$，可见 $E=e^D$ 或 $\Delta = e^D - I$，故

$$DF(x) = (D/(e^D - I))f(x) = \sum_k B_k D^k f(x)/k!.$$

由此

$$F(x) = \int f(x)dx + \sum_{k\geq 1} (B_k f^{(k-1)}(x)/k!),$$



$$\sum_{k=1}^{n} f(k) = F(n+1) - F(0)$$

$$= \int_1^{n+1} f(x)dx + \sum_{k \geq 1} B_k f^{(k-1)}$$

$$\times (n+1)/k! + C.$$

启发性推导至此完成，上式中不含余项. 下面我们用归纳法来严格地证明(8)式.

首先，应用分部积分公式可得

$$\int_k^{k+1} (\{x\} - (1/2))f'(x)dx$$

$$= (x - k - 1/2)f(x) \Big|_k^{k+1} - \int_k^{k+1} f(x)dx$$

$$= (f(k+1) - f(k))/2 - \int_k^{k+1} f(x)dx.$$

分别令 $k = 1, 2, \cdots, n-1$, 然后相加即得

$$\int_1^n (\{x\} - (1/2))f'(x)dx$$

$$= \sum_{k=1}^{n-1} f(k) + (f(n) - f(1))/2 - \int_1^n f(x)dx.$$

但 $B_1 = -1/2$, $B_1(x) = x - 1/2$, 故上式可写成

$$\sum_{k=1}^{n-1} f(k) = \int_1^n f(x)dx - (f(n) - f(1))/2$$

$$+ \int_1^n B_1(\{x\})f'(x)dx.$$

此即 $m = 1$ 时的(8)式. 今归纳假设 (8) 式成立，应用分部积分公式于 R_m, 利用命题 11, 并注意到 $B_m(0) = B_m(1) = B_m$, 可见 $B_m(\{x\})$ 为 x 的连续函数，于是

$$((-1)^{m+1}/m!) \int_1^n B_m(\{x\})f^{(m)}(x)dx$$

$$= ((-1)^{m+1}/(m+1)!)(B_{m+1}(1)f^{(m)}(n)$$



$$
\begin{aligned}
&- B_{m+1}(0)f^{(m)}(1)) \\
&- ((-1)^{m+2}/(m+1)!) \\
&\times \int_1^n B_{m+1}(\{x\})f^{(m+1)}(x)dx \\
= &((-1)^{m+1}B_{m+1}/(m+1)!)(f^{(m)}(n) \\
&- f^{(m)}(1)) - ((-1)^{m+2}/(m+1)!) \\
&\times \int_1^n B_{m+1}(\{x\})f^{(m+1)}(x)dx.
\end{aligned}
$$

但 $B_{2p+1}=0$ $(p\geqslant 1)$，故当 $m\geqslant 1$ 时，$(-1)^{m+1}B_{m+1}=B_{m+1}$，所以

$$
\begin{aligned}
R_m = &(B_{m+1}/(m+1)!)(f^{(m)}(n)-f^{(m)}(1)) \\
&+ ((-1)^{m+2}/(m+1)!)\int_1^n B_m(\{x\})f^{(m+1)}(x)dx.
\end{aligned}
$$

代入(8)式可见该式把 m 换为 $m+1$ 后依然成立，归纳证毕.

对于余项 R_m，我们注意到由命题 11，易将 $B_{2m}(\{x\})$ 展成 Fourier 级数

$$
\begin{aligned}
B_{2m}(\{x\}) = &2(2m)!(2\pi)^{-2m}(-1)^{m+1} \\
&\times \sum_{k=1}^{\infty} k^{-2m}\cos(2k\pi x),
\end{aligned}
\tag{10}
$$

故

$$
\begin{aligned}
|B_{2m}(\{x\})| \leqslant |B_{2m}| = &2(2m)!(2\pi)^{-2m} \\
&\times \sum_{k=1}^{\infty} k^{-2m} < 4(2\pi)^{-2m}(2m)!.
\end{aligned}
$$

上述不等式亦可从命题 5，命题 1 及命题 3 推出. 由此不等式可见

$$
|B_{2m}(\{x\})/(2m)!| < 4(2\pi)^{-2m}.
$$

因此只要 $f^{(m)}(x)$ 之增长不过于迅速，余项 R_m 通常很小.



第三章 反演技巧

3.1. 重排问题与环状字计数

在代数及分析问题中，为了定出某个未知元，我们常从问题的要求出发列出未知元所满足的一类方程，然后从中解出未知元本身．这一过程同样适用于组合计数问题．设 $f(n)$ 为某个计数问题的解，我们首先设法求出 $f(n)$ 所满足的关系式

$$\sum_{r=1}^{n} c_{n,r} f(r) = g(n), \tag{1}$$

然后从中解出

$$\sum_{r=1}^{n} d_{n,r} g(r) = f(n). \tag{2}$$

(1)与(2)两式即称为反演公式．

例 1 (**重排问题**)． 在 n 个文字 $1, 2, \cdots, n$ 形成的 $n!$ 个排列 $a_1a_2\cdots a_n$ 中，满足 $a_i \neq i$ $(i = 1, 2, \cdots, n)$ 的排列有多少个？这一问题也可叙述成：有 n 个人坐在 n 个不同的座位上，今重新安排各人的座位，使每人不致回到原先的座位上，问有多少种重排方式？

例如当 $n = 4$ 时共有 9 个这样的排列．

2143　2341　2413　3142　3412

3421　4123　4312　4321

而如 4132，因 $a_3 = 3$，不属此种类型．



今以 D_n 记问题的解. 易见 $\binom{n}{r}D_{n-r}$ 为恰有 r 个 $a_i=i$ 的排列 $(a_1, a_2, \cdots, a_n)$ 之个数,既然全部排列个数为 $n!$,当有

$$\sum_{r=0}^{n}\binom{n}{r}D_{n-r}=n!.$$

应用后面的二项式反演公式便可解出

$$D_n=\sum_{r=0}^{n}(-1)^r\binom{n}{r}(n-r)!$$

$$=n!\sum_{r=0}^{n}(-1)r/r! \tag{3}$$

命题 1. (二项式反演公式).

$$a_n=\sum_{k=0}^{n}\binom{n}{k}b_k \Longleftrightarrow b_n=\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}a_k. \tag{4}$$

证. $$\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}a_k=\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}\sum_{i=0}^{k}\binom{k}{i}$$

$$\times b_i=\sum_{i=0}^{n}\left(\sum_{k=i}^{n}(-1)^{n-k}\binom{n}{k}\binom{k}{i}\right)b_i$$

$$=\sum_{i}\delta_{n,i}b_i=b_n.$$

注. 设 a_n 与 b_n 的指数生成函数分别为 $A(x)$ 及 $B(x)$, 则由乘法公式 (2.2.7) 可见 (4) 式实即 $A(x)=B(x)e^x \Longleftrightarrow B(x)=A(x)e^{-x}$ 的另一种表示形式.

作为另一个经典的反演公式乃数论中有名的 Möbius 反演公式:

命题 2.

$$f(n)=\sum_{d|n}g(d) \Longleftrightarrow g(n)=\sum_{d|n}\mu(n/d)f(d). \tag{5}$$



$d|n$ 表示和式遍及 n 的所有因子 d，而 $\mu(m)$ 为 Möbius 函数，它定义为

$$\mu(m) = \begin{cases} 1, & m = 1; \\ (-1)^k, & m = p_1p_2\cdots p_k，\text{其中 } p_i \geqslant 2 \text{ 为互异的素数}; \\ 0, & \text{其他情形}. \end{cases} \tag{6}$$

此命题可从第三节中更一般的结果推出，也可直接证明如下：首先由 $\mu(d)$ 定义可证

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{若 } n = 1; \\ 0, & \text{若 } n > 1. \end{cases}$$

此式等价于

$$\sum_{\substack{n \\ d|n|m}} \mu(m/n) = \delta_{dm}. \tag{7}$$

由此

$$\sum_{\substack{n \\ n|m}} \sum_{\substack{d \\ d|n}} g(d)\mu(m/n) = \sum_{\substack{d \\ d|m}} g(d) \sum_{\substack{n \\ d|n|m}} \mu(m/n) = g(m).$$

Möbius 反演公式的上述证明并不困难，重要的是它是如何推导出来的。在 Berlekamp [37] 中给出了由(5)的第一式逐次解出 $g(n)$ 的过程，从中自然地引出了 Möbius 函数，这种启发性的推理值得有兴趣的读者参考。Möbius 反演公式在组合计数、数论、信息论等问题中有重要的应用。作为例子，我们考察著名的环状字问题。

例 2 (**环状字计数问题**)。从有 m 个字母的字母表 $T = \{a, b, c, \cdots, s\}$ 中取出 n 个字母(允许重复)按顺时针方向排成圆环状

$$a_1a_2a_3\cdots a_na_{n+1}\cdots \quad (a_{n+i} = a_n).$$

此时称 $W = a_1a_2\cdots a_n$ 为一个长为 n 的环状字。由于一个



环状排列可以选取其中任一文字为 a_1，故 $a_1a_2\cdots a_n$ 与 $a_2\cdots a_na_1$，$a_3\cdots a_1a_2$ 等都看作是同一环状字。例如当 $m=2$，$n=4$，$T=\{a,b\}$ 时，计有6个环状字

$$aaaa,\ bbbb;\ abab;\ aabb,\ aaab,\ bbba.$$

这里环状字 $aabb$ 也可写成 $abba$ 或 $bbaa$。

今求环状字个数 $C_m(n)$。首先我们注意到由 m 种字母共可作出 m^n 个可重复的排列 $a_1a_2\cdots a_n$，它与环状字的唯一区别在于首尾不相接，亦即是“线状”的。n 个线状排列

$$a_1a_2\cdots a_n,\ a_2\cdots a_n,\ \cdots,\ a_na_1\cdots a_{n-1} \tag{8}$$

一旦首尾相接均对应同一个环状字 $a_1a_2\cdots a_n$。由此似乎有 $C_m(n)=m^n/n$? 但简单的例子 $m=2$，$n=4$ 指出 $C_2(4)=6\neq 4=2^4/4$。究其原因，原来 n 个线状排列(8)并不总是互异的。例如环状字 $a_1a_2a_3a_4=abab$ 只对应于二个（线状）排列 $abab$ 与 $baba$。若再细察一步便可明白，导致这种对应个数少于 $n=4$ 的原因在于这一字有“周期”2：$a_i=a_{i+2}$。于是我们定义：一个环状字 $W=a_1a_2\cdots a_na_{n+1}\cdots$ $(a_{n+i}=a_i)$，若存在正整数 p 使得 $a_i=a_{i+p}$ $(i=1,2,\cdots)$，则称 W 有周期 p。最小的 p 称为 W 的元周期。易证每一周期必为元周期的倍数。特别由 $a_{n+i}=a_n$ 可见 n 必为 p 的倍数。一个元周期为 p 的环状字显然对应于 p 个不同的（线状）排列，故若记 $M(p)=M_m(p)$ 为有元周期 p 的环状字个数，则必有

$$\sum_{p|n} pM(p)=m^n.$$

应用反演公式(5)即得

$$pM(p)=\sum_{q|p}\mu(p/q)m^q. \tag{9}$$

由此



$$C_m(n) = \sum_{p|n} M(p) = \sum_{p|n} (1/p) \sum_{q|p} \mu(p/q)m^q. \quad (10)$$

此式若引用 Euler ϕ 函数(见 3.4 节)可改写成单重和式(见(5.1.16)式).

这一问题可推广以用来解决信息论中"无逗号编码"问题.所谓"无逗号编码"乃指一个由长度为 n 的字构成的集合 C,任取其中两个字,要求对满足 $1 \leqslant k \leqslant n$ 的任一整数 k,头一个字的后面 $n-k$ 个字母与第二个字的前面 k 个字母不致构成集合 C 中另一字. 由此种性质可见,将此种字一个接一个发送出去时,两个字之间毋须加上逗号以示分隔,无逗号编码的一个中心问题就是使集合 C 中的字尽可能地多.

例 2 中的数 $M(p)$ 还联系到纠错编码理论中的"**有限域上不可约多项式之计数问题**"(见 Berlekamp [37]):设 $GF(p)$ 为具有 p 个元的有限域, p 为素数. 一个 $GF(p)$ 上的多项式 $f(x) = \sum a_i x^i$, $a_i \in GF(p)$, 若除去常数及 f 自身外别无因式,则称为不可约.在有限域理论中证明了(见万哲先[2]):所有最高次项系数为 1, 次数 ∂f 除尽 n 的不可约多项式 $f(x)$ 之积等于 $x^{p^n} - x$:

$$x^{p^n} - x = \prod_{\partial f|n} f(x). \quad (11)$$

今要求定出 $GF(p)$ 上最高次项系数为 1 的 n 次不可约多项式的个数 $U_p(n)$. 为此由(11)式见

$$p^n = \sum_{d|n} dU_p(d). \quad (12)$$

由反演公式(5)即知

$$nU_p(n) = \sum_{d|n} \mu(n/d)p^d.$$

因而

$$U_p(n) = (1/n) \sum_{d|n} \mu(n/d)p^d. \quad (13)$$

与(9)式比较可见 $U_p(n) = M_p(n)$. 例如取 $p=2$, $n=4$,



可见 $GF(2)$ 上 4 次不可约多项式共有

$$U_2(4)=(1/4)(-2^2+2^4)=3$$

个，它们是

$$x^4+x^3+1,\ x^4+x+1,\ x^4+x^3+x^2+x+1.$$

在(13)式的证明中我们利用了关系式(11)，在 Berlekamp [37] 中直接从任一多项式必可分解成不可约多项式之积这一更简单的事实出发，运用生成函数方法证得(13)，且得到了更多的结果，此处不再细述了.

3.2. 第一反演公式

3.2.1. 第一反演公式

反演公式(3.1.1)与(3.1.2)等价于相应的系数阵 $C=(c_{ij})$ 与 $D=(d_{ij})$ 互逆，因此，只要我们能构造出二个互逆的三角阵，就能写出相应的反演公式. 下面的命题即给出了构造两个互逆阵的方法.

命题 1. 设 $\{p_n(x)\}$ 与 $\{q_n(x)\}$ 为两列多项式，其中 $p_k(x)$ 与 $q_k(x)$ 为 k 次多项式，若

$$p_n(x)=\sum_k c_{n,k}q_k(x),\quad q_n(x)=\sum_k d_{n,k}p_k(x),\qquad (n=0,1,2,\cdots)\tag{1}$$

则

$$a_n=\sum_k c_{n,k}b_k \Longleftrightarrow b_n=\sum_k d_{n,k}a_k.$$

$$(n=0,1,2,\cdots)\quad (n=0,1,2,\cdots)\tag{2}$$

证. 记向量 $p(x)=(p_i(x))_{i=0}^n$，$q(x)=(q_i(x))_{i=0}^n$，则(1)式等价于

$$p(x)=Cq(x),\quad q(x)=Dp(x).$$



其中 $C=(c_{n,k})$, $D=(d_{n,k})$. 因此 $p(x)=CDp(x)$,于是 $CD=I$, I 为 $n+1$ 阶单位阵.

作为命题 1 的应用,取 $p_n(x)=x^n$, $q_n(x)=(x-1)^n$, 则由二项式定理

$$(x-1)^n=\sum\binom{n}{i}(-1)^{n-i}x^i,$$

$$x^n=(x-1+1)^n=\sum\binom{n}{i}(x-1)^i.$$

可见 $\{x^n\}$ 与 $\{(x-1)^n\}$ 间关系式(1)成立,由此即推出二项式反演公式(3.1.1).

命题 2 (Stirling 反演公式).

$$a_n=\sum S(n,k)b_k \Longleftrightarrow b_n=\sum s(n,k)a_k. \tag{3}$$

证　取 $p_n(x)=x^n$, $q_n(x)=[x]_n$, 由 (2.4.3) 及命题 1 即得证.

作为命题 1 应用的第三个例子,我们注意到 $[-x]_n=(-1)^n[x]^n$ 乃 x 的多项式,故必可展开成

$$[-x]_n=\sum L(n,k)[x]_k. \tag{4}$$

在此式中以 $-x$ 代 x 便得

$$[x]_n=\sum L(n,k)[-x]_k. \tag{5}$$

由此推出

命题 3 (Lah 反演公式).

$$a_n=\sum_k L(n,k)b_k \Longleftrightarrow b_n=\sum_k L(n,k)a_k. \tag{6}$$

为导出 $L(n,k)$ 的显式,我们注意由(1.2.17),有

$$[m]^n/n!=\sum_{k=0}^{n}\binom{m}{k}\binom{n-1}{k-1},$$

因此



$$[m]^n = \sum_{k=0}^{n} (n!/k!) \binom{n-1}{k-1} [m]_k,$$

或

$$[-m]_n = (-1)^n [m]^n = \sum_{k=0}^{n} \times (-1)^n (n!/k!) \binom{n-1}{k-1} [m]_k.$$

所以

$$L(n, k) = (-1)^n (n!/k!) \binom{n-1}{k-1}. \tag{7}$$

同样,由命题(2.5.5)及命题(2.5.9)推出

命题 4 (Bernoulli 反演公式).

$$a_n = \sum \binom{n}{k} (n-k+1)^{-1} b_k \Leftrightarrow b_n = \sum \binom{n}{k} B_{n-k} a_k.$$

其中 B_j 为 Bernoulli 数.

为了应用命题 1 来推出反演公式,我们须将一个多项式 $p(x)$ 按给定的列 $\{q_n(x)\}$ 展开: $p(x) = \sum_n c_n q_n(x)$. 当 $q_n(x) = x^n$ 时,即通常的 Taylor 展开

$$p(x) = \sum (D^n p(x)/n!)_{x=0} x^n.$$

容易看到,对 $q_n(x) = x^n$,上述展开式得以成立的原因在于 $Dq_n(x) = nq_{n-1}(x)$, $q_0(x) = 1$ 及 $q_n(0) = 0 (n \geqslant 1)$. 由此引出下列定义

定义 1. 若多项式列 $\{p_n(x)\}$ 满足条件: (i) $p_n(x)$ 为 n 次多项式; (ii) $p_0(x) = 1$, $p_n(0) = 0$ $(n \geqslant 1)$, 则称 $\{p_n(x)\}$ 为正规多项式列.

定义 2. 对于给定的多项式列 $\{p_n(x)\}$,若线性算子 P 满足条件: (i) $Pp_0(x) = 1$; (ii) $Pp_n(x) = np_{n-1}(x)$ $(n >$



0)，则称 P 为 $\{p_n(x)\}$ 的基本算子。反之，对给定的算子 P，满足所述 (i) 与 (ii) 的多项式列称为 P 的基本列。

命题 5. 对每个正规多项式列，存在唯一的基本算子 P。

实际上，由 $p_n(x)$ 的正规性易知每个 n 次多项式 $\varphi(x)$ 可唯一地写成 $\varphi(x)=\sum\limits_{i=0}^{n}a_ip_i(x)$，因此 $P\varphi(x)=\sum\limits_{k=1}^{n}ka_k\times p_{k-1}(x)$。算子 P 即为此式所唯一确定。

命题 6. 若 $\{p_n(x)\}$ 为正规多项式列，它的基本算子为 P，则对任一 n 次多项式 $\varphi(x)$，必有

$$\varphi(x)=\sum_{k=0}^{n}(P^k\varphi(x)/k!)_{x=0}\,p_k(x). \tag{8}$$

证．在 $\varphi(x)=\sum c_kp_k(x)$ 两边施以算子 P^k，然后令 $x=0$ 即得

$$(P^k\varphi(x))_{x=0}=\sum_{i=0}^{n}c_i[i]_kp_{i-k}(0)=c_kk!.$$

由此即推出(8)式。

例 1．对 $p_n(x)=x^n$，其基本算子 P 即微分算子 D，此时(8)即 Taylor 展式。

例 2．对 $p_n(x)=[x]_n$，此时 $P=\Delta$，于是

$$\varphi(x)=\sum(\Delta^k\varphi(x)/k!)[x]_k,$$

而

$$(\Delta^k\varphi(x))_{x=0}=((E-I)^k\varphi(x))_{x=0}$$
$$=\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}\varphi(i).$$

例 3．对 $p_n(x)=[x]^n$，$P=\nabla$ 为向后差分算子：$\nabla f(x)=f(x)-f(x-1)$。因易证 $\nabla[x]^n=n[x]^{n-1}$，于是

$$\varphi(x)=\sum_{k}(\nabla^k\varphi(x)/k!)_{x=0}[x]^k, \tag{9}$$



而

$$(\nabla^k\varphi(x))_{x=0}=((I-E^{-1})^k\varphi(x))_{x=0}$$
$$=\sum_{i=0}^{k}\binom{k}{i}(-1)^i\varphi(-i).$$

注意,若将 $(x+y)^n$, $[x+y]_n$ 与 $[x+y]^n$ 视为 x 的函数分别按相应的基本算子 D,Δ与∇作 Taylor 式展开(8),可得出

$$(x+y)^n=\sum\binom{n}{k}x^ky^{n-k},$$

$$[x+y]_n=\sum\binom{n}{k}[x]_k[y]_{n-k}, \tag{10}$$

$$[x+y]^n=\sum\binom{n}{k}[x]^k[y]^{n-k}. \tag{11}$$

此种多项式列称作是二项式型多项式，我们将在下一小节中论及.

由命题 6 及命题 1 即可推出下面的

定理 A. 设 $\{p_n(x)\}$ 与 $\{q_n(x)\}$ 为两个正规多项式列,相应的基本算子分别为 P 与 Q,则

$$a_n=\sum_{k=0}^{n}(Q^kp_n(x)/k!)_{x=0}b_k$$
$$\Longleftrightarrow b_n=\sum_{k=0}^{n}(P^kq_n(x)/k!)a_k. \tag{12}$$

例如取 $p_n(x)=x^n$, $q_n(x)=[x]_n$, $P=D$, $Q=\Delta$ 即为 Stirling 公式(3).

3.2.2. 二项式型的多项式列

当正规列 $\{p_n(x)\}$ 给定后,它的基本算子为命题 5 所完全确定;反之,当算子 P 给定后,又如何寻求相应的基本列?



Mullin 与 Rota 对一类特殊的算子解决了这一问题。他们详细地研究了一类称之为二项式型的多项式列，得出了一系列有用的结果。下面我们引述其中的主要结果，并举例加以说明。详细的推证可参阅 Aigner [19].

定义 3. 满足下列两条件的多项式列称为二项式型多项式：

(i) $p_0(x) = 1$;

(ii) $p_n(x+y) = \sum_{k=0}^{n}\binom{n}{k}p_k(x)p_{n-k}(y)$. $\qquad$ (13)

由(10)及(11)式知 $x^n, [x]_n$ 及 $[x]^n$ 均为二项式型多项式。注意由上述定义之 (ii) 可见，$p_n(0) = 0$ $(n > 1)$，亦即二项式型的多项式列必为正规列。下列定理给出了二项式型多项式的一个特征。

命题 7. $\{p_n(x)\}$ 为二项式型多项式列的充要条件是，它的基本算子 P 满足 (i) $PE^a = E^aP$，亦即 P 与移位算子 $E^af(x) = f(x+a)$ 可交换，其中 a 为任意实数；(ii) $Px = c \neq 0$。

满足上述条件 (i) 与 (ii) 的算子称作 δ 算子。

命题 8. 任一 δ 算子必可展成微分算子 D 的幂级数：

$$P = \sum_{k\geq 0} a_k D^k/k!.$$

其中 $a_k = (Px^k)_{x=0}$。

例如 $E^a = e^{aD} = \sum a^kD^k/k!$；$\Delta = e^D - I$，$\nabla = I - e^{-D}$ 等等。

对于 δ 算子 $P = \sum_{k\geq 0} a_k D^k/k!$，定义其导算子为

$$P' = \sum_{k\geq 1} a_k D^{k-1}/(k-1)!.$$

例如 $D' = I$ (恒等算子)，$(E^a)' = (e^{aD})' = ae^{aD} = aE^a$，



$\Delta' = e^D = E, \nabla' = e^{-D} = E^{-1}$ 等等.

下面的定理给出了由 δ 算子构造相应的基本列的方法.

定理 B. 设 $P = DT$ 为 δ 算子,则其基本列为

(i) $p_0(x) = 1,\ p_n(x) = xT^{-n}x^{n-1} \qquad (n > 0)$,

(ii) $p_0(x) = 1,\ p_n(x) = x(P')^{-1}p_{n-1}(x)$.

此处 (ii) 由递推方式给出.

例 1. 对 Abel 算子 $P = DE^a$, 它显然为 δ 算子,于是相应的基本列(由 (i))为

$$p_n(x) = xE^{-an}x^{n-1} = x(x - an)^{n-1}. \tag{14}$$

这一多项式称作 **Abel 多项式.** 由命题 7, 它必为二项式型多项式,从而必有

$$\begin{aligned}(x + y)(x + y - an)^{n-1} &= \sum_{k=0}^{n}\binom{n}{k}x(x - ak)^{k-1} \\ &\quad \times y(y - a(n - k))^{n-k-1}.\end{aligned} \tag{15}$$

例 2. $P = \Delta$, 此时 $P' = E$, 故由 (ii)

$$\begin{aligned}p_n(x) &= xE^{-1}p_{n-1}(x) = xp_{n-1}(x - 1) \\ &= x(x - 1)p_{n-2}(x - 2) = \cdots = [x]_n.\end{aligned}$$

同样对于 $P = \nabla$, $p_n(x) = xEp_{n-1}(x) = xp_{n-1}(x + 1) = \cdots = [x]^n$.

例 3. **Laguerre 算子** $Lf(x) = -\int_0^\infty e^{-t}f'(x + t)dt$,

亦即

$$\begin{aligned}L &= -\int_0^\infty e^{-t}e^{tD}D\,dt = -e^{-t(I-D)}D/D - I\Big|_0^\infty \\ &= D/(D - I) = D(I/D - I).\end{aligned}$$

故由 (i) 相应的基本列为

$$L_n(x) = x(D - I)^n x^{n-1}$$



$$= x\sum_{k=0}^{n}(-1)^k\binom{n}{k}D^{n-k}x^{n-1}$$

$$= \sum_{k=1}^{n}(-1)^k(n!/k!)\binom{n-1}{k-1}x^k. \qquad (16)$$

$L_n(x)$ 可以写成另一种更紧凑的形式，因 $D-I=e^xDe^{-x}$，故 $(D-I)^n=e^xD^ne^{-x}$，由此

$$L_n(x)=xe^x(d/dx)^n(e^{-x}x^{n-1}). \qquad (17)$$

由命题 7 可见 $L_n(x)$ 为二项式型多项式.

定理 C. 设 $P=P(D)$ 为一 δ 算子，其基本列为 $\{p_n(x)\}$，则与 P 的逆算子 $P^{(-1)}$ 相应的基本列为

$$q_n(x)=\sum_k(P^kx^n/k!)_{x=0}x^k.$$

注. 此处 $P(D)$ 的逆算子 $P^{(-1)}(D)$ 定义为 $P^{(-1)}(P(D))=D$，亦即 $P^{(-1)}(x)$ 为 $P(x)$ 的反函数. 例如对于 $y=e^x-1$，其反函数 $x=\log(1+y)$，于是 $\Delta=e^D-I$ 的逆算子 $\Delta^{(-1)}$ 为 $\log(I+D)$. 又如 $y=x/(x-1)$，其反函数 $x=y/(y-1)$，故 Laguerre 算子 $L=D/(D-I)$ 的逆算子 $L^{(-1)}$ 为自身.

例. 对 $\Delta=e^D-I$，其逆算子 $\Delta^{(-1)}=\log(I+D)$，故 $\Delta^{(-1)}$ 的基本列为

$$e_n(x)=\sum_{k=0}^{n}(\Delta^kx^n/k!)_{x=0}x^k$$

$$=\sum_{k=0}^{n}S(n,k)x^k. \qquad (18)$$

命题 9. 设 $\{p_n(x)\}$ 为二项式型多项式列，其基本算子 $P=P(D)$，则有

$$\sum_n p_n(x)u^n/n! = \exp(xp^{(-1)}(u)).$$



例 1. 对于 $P = \log(I + D)$，即得

$$\sum_n e_n(x)u^n/n! = \exp(x(e^u - 1)).$$

尤令 $x = 1$，及(18)式，即得

$$\sum_n Y_n u^n/n! = \exp(e^u - 1).$$

例 2. 对 Laguerre 算子 $L = D/(D - I) = L^{(-1)}$，$L_n(x)$ 如(16)式所示，于是

$$\sum_n L_n(x)u^n/n! = \exp(xu/(u - 1)).$$

定理 D. 设 $\{p_n(x)\}$ 与 $\{q_n(x)\}$ 为两个二项式型多项式列，它们的基本算子分别为 $P = P(D)$，$Q = Q(D)$，且 $q_n(x) = \sum_k c_{n,k} p_k(x)$，则 $r_n(x) = \sum_k c_{n,k} x^k$ 亦为一二项式型多项式列，它的基本算子 $R = Q(P^{(-1)}(D))$.

例 1. 由 $x^n = \sum S(n, k)[x]_k$，取 $P(D) = \Delta$，$Q(D) = D$，于是 $Q(P^{(-1)}(D)) = \Delta^{(-1)} = \log(I + D)$. 应用上述定理可见 $\sum S(n, k)x^k$ 亦为二项式型多项式，它的基本算子为 $\log(I + D)$.

例 2. 由 $[x]^n = \sum \bar{L}(n, k)[x]_k$，此时 $P(D) = \Delta$，$Q(D) = \nabla = I - e^{-D}$，于是 $P^{(-1)}(D) = \Delta^{(-1)} = \log(I + D)$，$Q(P^{(-1)}(D)) = I - \exp(-\log(I + D)) = I - (I + D)^{-1} = D(I + D)^{-1}$，故由本定理 $r_n(x) = \sum \bar{L}(n, k)x^k$ 的基本算子为 $D(I + D)^{-1}$，而由定理 B，

$$\begin{aligned} r_n(x) &= x(I + D)^n x^{n-1} \\ &= x\sum_{k=0}^{n} \binom{n}{k} D^{n-k} x^{n-1} \\ &= \sum_{k=0}^{n} \binom{n}{k} [n - 1]_{n-k} x^k \end{aligned}$$



$$= \sum_{k=1}^{n} (n!/k!) \binom{n-1}{k-1} x^k.$$

亦即 $[x]_n = (-1)^n[-x]^n = \sum (-1)^n (n!/k!) \binom{n-1}{k-1} [-x]_k$，与(7)式一致.

3.3. Möbius 反演公式

寻求一般形式的反演公式

$$f(n) = \sum_{0 \leqslant i \leqslant n} c(i, n) g(i),$$

$$g(n) = \sum_{0 \leqslant i \leqslant n} d(i, n) f(i), \tag{1}$$

归结为求三角阵 $C = (c(i, j))$ 的逆阵 $D = (d(i, j))$. 命题 (3.2.1) 给出了构造两个互逆的三角阵的一种有效的方法，但毕竟有其局限性. 其实对于任一三角阵 C，只要主对角线元 $c(i, i) \neq 0$，其逆阵可以用下面的递推方式求出：首先，由 $CD = I$ 得

$$\sum_{1 \leqslant k \leqslant n} c(i, k) d(k, j) = \delta(i, j), \tag{2}$$

其中 $\delta(i, j)$ 为 Kronecker 函数，

$$\delta(i, i) = 1, \ \delta(i, j) = 0 \ (i \neq j). \tag{3}$$

但对 $i > k$，$c(i, k) = 0$；对 $k > j$，$d(k, j) = 0$，故(2)式化作

$$\sum_{i \leqslant k \leqslant j} c(i, k) d(k, j) = \delta(i, j). \tag{4}$$

尤令 $i = j$，得 $c(i, i) d(i, i) = 1$，由此

$$d(i, i) = c(i, i)^{-1}. \tag{5}$$

而对 $j > i$，由 $\delta(i, j) = 0$ 及(4)式可见



$$d(i,j) = -c(i,i)^{-1} \sum_{i<k\leqslant j} c(i,k)d(k,j). \qquad (6)$$

(5),(6)两式给出了依次计算诸 $d(i,j)$ 的递推算法.

1964 年, Rota 首先注意到 (见 Rota [135]), 若将 (5), (6) 两式中出现的变元 i, j 看作是更一般集合 S 中的元, 关系式 $i<k\leqslant j$ 等看作是集合 S 中的一种更广泛意义下的顺序关系,则反演公式 (1) 能推广成更一般形式,从而建立一种形式统一的反演理论, 由此可以引出许多应用很广的反演公式来.

定义 1. 设在集合 S 上给出一种序关系$\leqslant$,它满足条件: 对任意的 $a, b, c\in S$, 下列三式成立:

(i) $a\leqslant a$; (ii) $a\leqslant b, b\leqslant a\Rightarrow a=b$; (iii) $a\leqslant b$, $b\leqslant c\Rightarrow a\leqslant c$;

则称 S 为一偏序集合. 此时, 对元 $a, b\in S$, 以 $[a, b]$ 记满足条件 $a\leqslant c\leqslant b$ 的元 $c\in S$ 之全体. 若对任二元 $a,b\in S$, $[a, b]$ 总为一有限集,则称 S 为局部有限的偏序集合.

例 1. $S=T=$\{所有的非负整数\}, "$\leqslant$" 取为通常的 "小于或等于".

例 2. $S=D=$\{所有的正整数\}, $a\leqslant b$ 定义为 a 除尽 b, 亦即 $a|b$.

例 3. 设 $N=\{1, 2, \cdots, n\}$, $S=\mathscr{B}=\{A|A\subseteq N\}$, 亦即由$N$的所有子集构成,对 $A, B\in S$, $A\leqslant B$ 定义为 $A\subseteq B$ (A 为 B 的子集).

容易验证上述三种集合关于所述的序关系构成局部有限的偏序集合.

注 1. 偏序集合 S 中的任二元 a, b 并不总是可以相互比较的,亦即可能 $a\leqslant b$ 与 $b\leqslant a$ 都不成立,例如上述例 2 中的 $a=3$ 与 $b=7$, 例 3 中的 $A=\{1, 3, 5\}$ 与 $B=$



$\{3,7\}$.但对例1;则任取 $a, b\in S$, 总有 $a\leqslant b$ 或 $b\leqslant a$.此种偏序集合称之为线性序集.

注2. 对于一个偏序集合 S 总可以假定其中有元0，满足

$$0\leqslant a \qquad (a\in S),$$

实际上若 S 中不存在此种元，总可以加入进去. 例如例1中的0，例2中的1，例3中的空集合 $\varnothing$ 等.

注3. 若 $a\leqslant b$, $a\neq b$, 则记作 $a<b$. 又 $a\leqslant b$ 也可记作 $b\geqslant a$,同样 $a<b$ 可写作 $b>a$.

今取 $\mathscr{F}$ 为定义于 $S\times S$ 上的满足下列条件的实值函数全体:

$$f(x, x)\neq 0;\ f(x,y)=0 \qquad (x\not\leqslant y).$$

此处 $x\not\leqslant y$ 表示 $x>y$ 或者 x 与 y 不可比较，又 f 也可以取值于任意域中. 对 $f(x, y)$ 的这一限制就如前面对三角阵 $(c(i, j))$ 之限制 $c(i, i)\neq 0$, $c(i, j)=0$ $(i>j)$. 同样与(4)式相仿,我们在 $\mathscr{F}$ 中引进"卷积"运算"$*$",

$$(f*g)(x, y)=\sum_{x\leqslant u\leqslant y} f(x, u)g(u, y). \qquad (7)$$

今证集合 $\mathscr{F}$ 关于运算$*$构成一个群,亦即下列命题成立:

命题1. 运算$*$满足结合律

$$(f*g)*h=f*(g*h). \qquad (8)$$

命题2. $\mathscr{F}$ 中存在单位元 δ, 满足 $(f*\delta)=f$. 此元 $\delta(x, y)$ 即为 Kronecker 函数

$$\delta(x,x)=1;\ \delta(x, y)=0\ (x\neq y). \qquad (9)$$

命题3. 对于任一元 $f\in\mathscr{F}$, 必有逆元 f^{-1} 满足

$$f^{-1}*f=\delta.$$

实际上,对固定的 x, $f^{-1}(x, y)$ 可按下列归纳方式定出(比较(5)与(6)):



(i) 若 $y=x$，则 $f^{-1}(x,y)=1/f(x,x)$；

(ii) 若 $y>x$，则 $f^{-1}(x,y)=(1/f(y,y))$

$$\times\sum_{x\leqslant u<y}f^{-1}(x,u)f(u,y);$$

(iii)若 $y\not\geqslant x$，则 $f^{-1}(x,y)=0$。 (10)

命题 1 之证明. $((f*g)*h)(x,y)$

$$=\sum_{x\leqslant u\leqslant y}(f*g)(x,u)h(u,y)$$

$$=\sum_{x\leqslant u\leqslant y}\left(\sum_{x\leqslant v\leqslant u}f(x,v)g(v,u)\right)h(u,y)$$

$$=\sum_{x\leqslant v\leqslant y}f(x,v)\sum_{v\leqslant u\leqslant y}g(v,u)h(u,y)$$

$$=\sum_{x\leqslant v\leqslant y}f(x,v)(g*h)(v,y)$$

$$=(f*(g*h))(x,y).$$

命题 2 之证明. 由 $\delta(x,y)$ 之定义知

$$(f*\delta)(x,y)=\sum_{x\leqslant u\leqslant y}f(x,u)\delta(u,y)=f(x,y).$$

命题 3 之证明. 首先我们注意由集 $\mathscr{F}$ 之假设知 $f(y,y)\neq 0$，故 $1/f(y,y)$有定义；又因满足 $x\leqslant u<y$ 的元 u 只有有限个，故 (ii) 中和式仅包含有限项，故由 (i) 至 (iii) 所定义的 $f^{-1}(x,y)$ 是确定的. 再证 $f^{-1}*f=\delta$. 实际上当 $x=y$ 时，

$$(f^{-1}*f)(x,x)=f^{-1}(x,x)f(x,x)=1.$$

而当 $x<y$ 时，由(10)式可见

$$(f^{-1}*f)(x,y)=\left[\sum_{x\leqslant u<y}f^{-1}(x,u)f(u,y)\right]$$

$$+f^{-1}(x,y)f(y,y)=0.$$

对于 $x\not\leqslant y$，由(10)式当有

$$(f^{-1}*f)(x,y)=0.$$



证毕。

注. 应用群论中的标准论证方法易证，若 $f^{-1}*f=\delta$，则 $f*f^{-1}=\delta$. 换言之，左逆必为右逆. 又逆元 f^{-1} 是唯一确定的，亦即若 $g*f=\delta$，则 $g=f^{-1}$.

由逆元的定义，若 $f=g*\alpha$，则 $g=f*\alpha^{-1}$. 故若记 $\alpha^{-1}=\beta$，$f(x)=f(0,x)$，$g(x)=g(0,x)$，则由运算 $*$ 的定义即见

$$f(x)=\sum_{0\leqslant u\leqslant x}\alpha(u,x)g(u)$$

$$\Longleftrightarrow g(x)=\sum_{0\leqslant u\leqslant x}\beta(u,x)f(u). \tag{11}$$

此式概括了一类广泛的反演公式，为了将经典的 Möbius 反演公式推广到一般情形，取 $\alpha(x,y)=\zeta(x,y)$，

$$\zeta(x,y)=1\ (x\leqslant y);\ \zeta(x,y)=0\ (x\nleqslant y).$$

这一函数称作 ζ 函数，其逆 $\zeta^{-1}(x,y)$ 称为 Möbius 函数，记作 $\mu(x,y)$. 由(10)式可见，$\mu(x,y)$ 可按下列法则算出：

$$\mu(x,x)=1,\ \mu(x,y)=-\sum_{x\leqslant u<y}\mu(x,u)\ (x<y). \tag{12}$$

于是由(11)式便推知下面的重要的反演公式。

定理 A (Möbius 反演定理). 设 S 为局部有限的偏序集，$f(x)$ 与 $g(x)$ 为定义于 S 上取值于某一域中的函数，则

$$f(x)=\sum_{0\leqslant u\leqslant x}g(u)\ (x\in S)$$

$$\Rightarrow g(x)=\sum_{0\leqslant u\leqslant x}\mu(u,x)f(u)\ (x\in S). \tag{13}$$

为了在各种特定的偏序集上导出具体的 Möbius 反演公式，我们需要计算相应的 Möbius 函数。下面的乘积定理给出了一种有用的计算方法，它使我们得以从简单的 Möbius 函数出发来合成复杂情形下的 Möbius 函数。



定义 1. 设 S_1 与 S_2 为两个局部有限的偏序集合，相应的偏序分别记作 $\leqslant_1$ 与 $\leqslant_2$，定义 S_1 与 S_2 的直积为

$$S = \{(a, b) \mid a \in S_1, b \in S_2\}.$$

S 上的偏序引出如下：对 $a = (a_1, a_2)$，$b = (b_1, b_2) \in S$，

$$a \leqslant b \quad \Longleftrightarrow a_1 \leqslant {}_1 b_1, \; a_2 \leqslant {}_2 b_2.$$

定理 B. 设 S_1, S_2 及 $S = S_1 \times S_2$ 如定义 1 所述，它们的 Möbius 函数分别为 μ_1, μ_2 与 μ，则

$$\mu((x_1, x_2), (y_1, y_2)) = \mu_1(x_1, y_1)\mu_2(x_2, y_2). \qquad (14)$$

其证见 Rota[135]。

下面我们给出若干特定的偏序集中反演公式(13)的表现形式. 为此我们首先引入局部有限偏序集合 S 的图示方法，此种图一般称作 **Hasse 图**，图中各点表示 S 中的元，而当 $x \leqslant y$ 时我们画出一条自 y 指向 x 的有向弧. 在这种形式下，由(12)式可见 $\mu(x, y)$ 的计算法则为：将位于从 y 到 x 的各条路上的点子(点 y 除外)之 $\mu(x, z)$ 值都加起来，然后变号，即得 $\mu(x, y)$。

例 1. $S = J(n) = \{0, 1, 2, \cdots, n\}$，$\leqslant$ 取为通常的序关系(小于等于)。S 的 Hasse 图如图 1 所示.

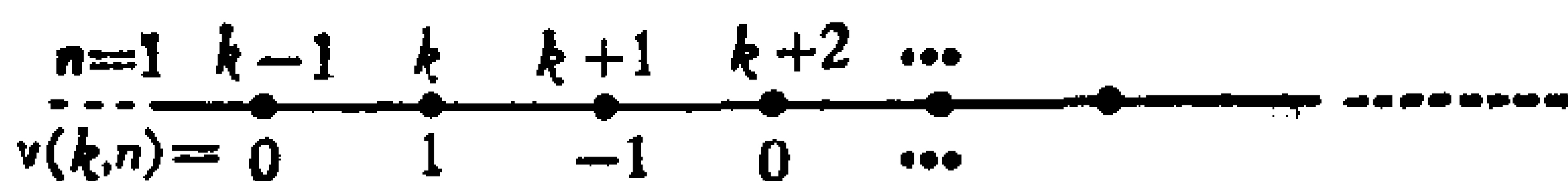


图 1.

此时从 n 到 k 的路只有一条，相应的 Möbius 函数易见为

$$\mu(k, n) = \begin{cases} 0, & n < k, n \geqslant k+2; \\ 1, & n = k; \\ -1, & n = k+1. \end{cases}$$



于是 $f(n)=\sum_{k=0}^{n} g(k)$ 的反演公式即为 $g(0)=f(0)$, $g(n)=f(n)-f(n-1)$, $(n\geq 1)$.

例 2. $S=D(n)=\{n$ 的所有因子$\}$. $a\leq b$ 表示 $a|b$. 它的 Hasse 图如图 2 所示.

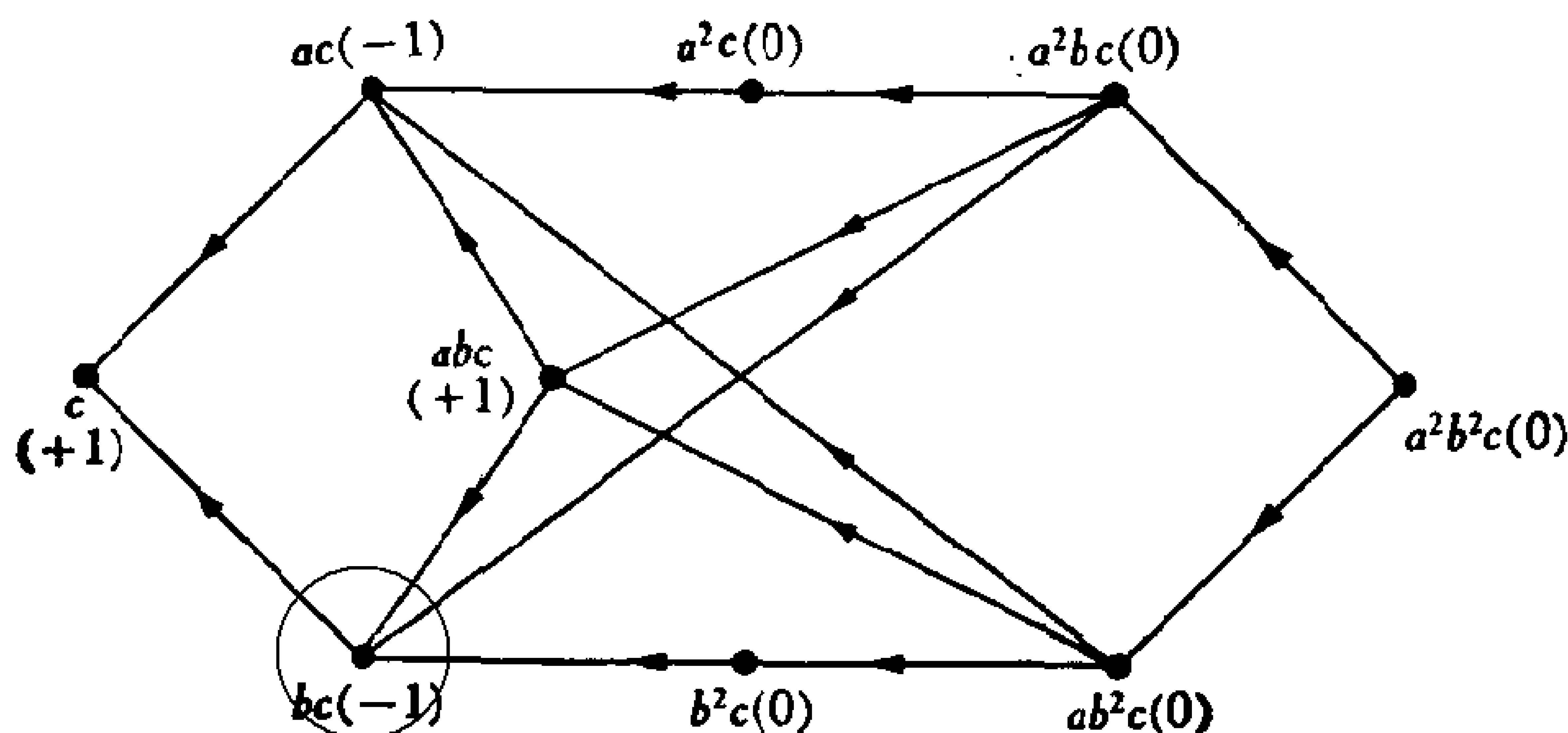


图 2.

我们用乘积定理导出此例的 Möbius 函数. 由素因子分解的唯一性可见, 若 $n=\Pi p_i^{\alpha_i}$, 则 $D(n)$ 与 $D(p_1^{\alpha_1})\times D(p_2^{\alpha_2})\times\cdots\times D(p_s^{\alpha_s})$同构. (注. 两个偏序集 S_1 与 S_2 间若存在一一对应: $x\in S_1\longleftrightarrow f(x)\in S_2$, 使得 $x\leq_1 y\Longleftrightarrow f(x)\leq_2 f(y)$, 则称 S_1 与 S_2 同构. 此时它们的 Möbius 函数间便有关系式 $\mu_1(x,y)=\mu_2(f(x),f(y))$.) 于是由乘积定理, 我们只需计算 $D(p^\alpha)$ 上的 Möbius 函数. 但 $D(p^\alpha)$ 由 1, p, p^2, $\cdots$, p^α 所组成, 故易见 $D(p^\alpha)$ 同构于 $J(\alpha)=\{0,1,\cdots,\alpha\}$, 因此

$$\mu(p^i,p^j)=\begin{cases}1, & i=j;\\ -1, & j-i=1;\\ 0, & \text{其他情形}.\end{cases}$$

由此可见



$$\mu\left(\prod_{i=1}^{s} p_i^{a_i},\ \prod_{i=1}^{s} p_i^{b_i}\right)$$

$$=\begin{cases}(-1)^{\Sigma(b_i-a_i)}, & \text{若对所有的 } i,\ b_i-a_i=0 \text{ 或 } 1;\\ 0, & \text{其他情形}.\end{cases}$$

此即

$$\mu(r,s)=\mu(s/r)$$

$$=\begin{cases}1, & \text{若 } r=s;\\ (-1)^k, & \text{若 } s/r \text{ 为 } k \text{ 个互异素数之积};\\ 0, & \text{其他情形}.\end{cases}$$

由此即导出经典的 Möbius 反演公式(3.1.5)。

例 3. 设集合N有 n 个元，$\mathscr{B}$ 由N的所有子集构成，其上的序关系取作集合的包含关系. 易证 $\mathscr{B}$ 与偏序集 $\sum_n=\{t \mid t=(t_1,\cdots,t_n),\ t_i=0 \text{ 或 } 1\}$ 同构，$\sum_n$ 上的偏序定义为 $t\leqslant r \Longleftrightarrow t_i\leqslant r_i,\ (i=1,2,\cdots,n)$. 实际上 $A\subseteq N$ 可对应于 $f(A)=(t_1,\cdots,t_n)$，其中 $t_i=1$ 当且仅当 $a_i\in A$ $(N=\{a_1,\cdots,a_n\})$. 此种对应显然为 $\mathscr{B}$ 与 $\sum_n$ 间的同构对应. 因此为了计算 $\mathscr{B}$ 的 Möbius 函数，我们只需计算 $\sum_n$ 上的 Möbius 函数. 但 $\sum_n=\sum_1\times\sum_1\times\cdots\times\sum_1$，而对于 $\sum_1$，$y\geqslant x$ 无非是 $y=x$ 或 $y=1,\ x=0$. 故 $\mu(x,y)=(-1)^{y-x}$. 应用乘积定理便得

$$\mu((x_1,\cdots,x_n),(y_1,\cdots,y_n))$$

$$=\prod_{i=1}^{n}\mu(x_i,y_i)=(-1)^{\Sigma y_i-\Sigma x_i}.$$

但当 $X,\ Y\in\mathscr{B}$ 与 $(x_1,\cdots,x_n)$，$(y_1,\cdots,y_n)$ 分别对应



时，$\sum x_i = |X|$，$\sum y_i = |Y|$，故

$$\mu(X, Y) = (-1)^{|Y|-|X|}.$$

由此导出重要的反演公式：

命题 4. $f(X) = \sum_{Y \subseteq X} g(Y)$

$$\Rightarrow g(X) = \sum_{Y \subseteq X} (-1)^{|X|-|Y|} f(Y). \qquad (15)$$

注．若我们改用 $X \supseteq Y$ 作为 $X \leqslant Y$ 的定义，则同样可以推知

$$f(X) = \sum_{Y \supseteq X} g(Y) \Rightarrow g(X) = \sum_{Y \supseteq X} (-1)^{|Y|-|X|} f(Y). \quad (16)$$

例 4．集合 A 的一个分划 π 是指(见定义(2.4.2))：$A = \bigcup_i A_i$，$A_i \neq \varnothing$，$A_i \cap A_j = \varnothing$ $(i \neq j)$．一个 n 元的集合共有 Y_n 种不同的分划(命题(2.4.10))，这些分划的全体构成的集合记作 $\Gamma(A)$．对于 $\Gamma(A)$ 中两种不同的分划 $\pi_1: A = \bigcup_i A_i$ 与 $\pi_2: A = \bigcup_j B_j$，若分划 π_1 是 π_2 的“加细”，则记作 $\pi_1 \leqslant \pi_2$．所谓“加细”乃指每个 B_j 由若干个 A_i 组成，亦即若 $A_i \cap B_j \neq \varnothing$，则 $A_i \subseteq B_j$．例如 $\pi_1 = \{\{a, b\}, \{c\}, \{d, e\}\} \leqslant \pi_2 = \{\{a, b\}, \{c, d, e\}\}$．易证 $\Gamma(A)$ 关于此种

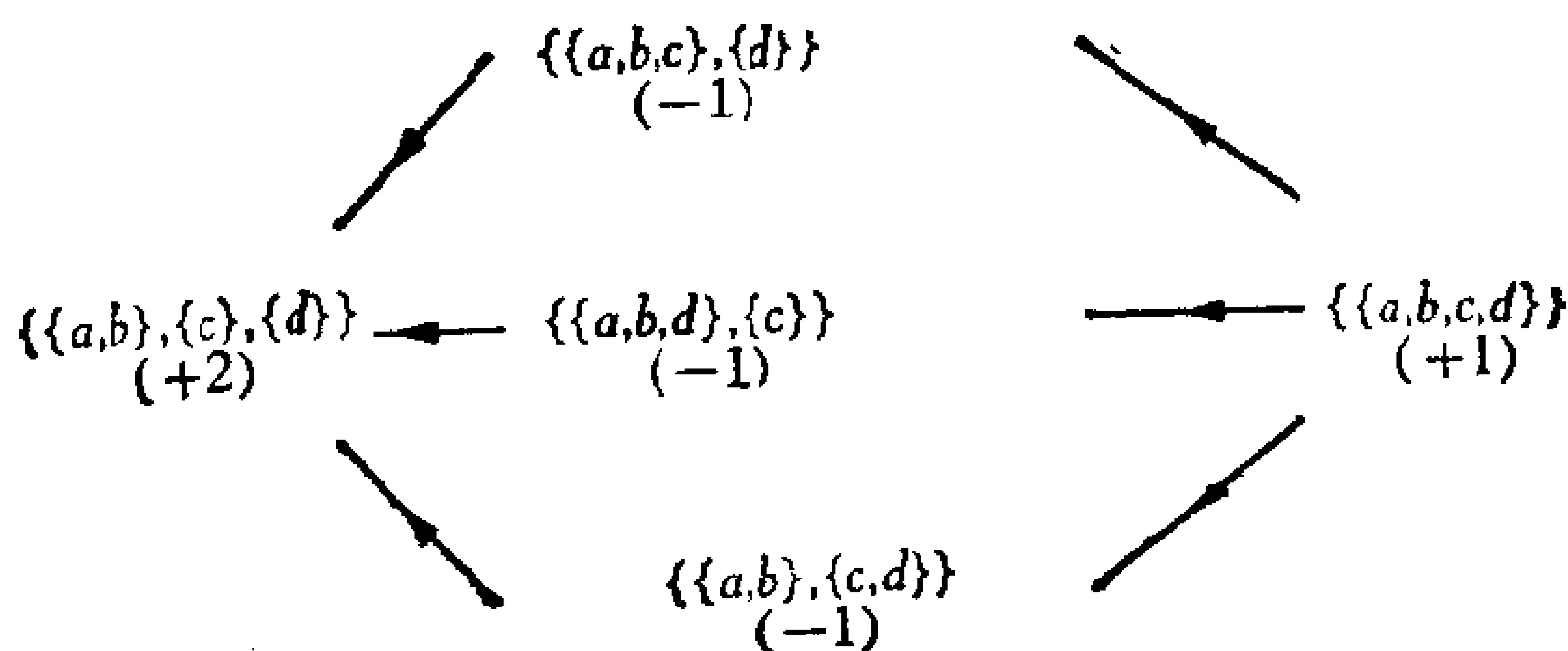


图 3.



偏序构成局部有限的偏序集. $\Gamma(A)$ 的 Hasse 图如图 3 所示.

对于 $\Gamma(A)$ 上的 Möbius 函数下面的命题成立:

命题 5. 设分划 π_1: $A=\bigcup_{i=1}^{p} A_i$, π_2: $A=\bigcup_{j=1}^{q} B_j$, $\pi_1 \leqslant \pi_2$, 若每个 B_j 由 n_j 个 A_i 组成, 则

$$\mu(\pi_1, \pi_2)=(-1)^{q+n_1+\cdots+n_q} \times (n_1-1)!(n_2-1)!\cdots(n_q-1)!. \qquad (17)$$

其证亦可由乘积定理得出, 但证明稍为长些, 见 Bender and Goldman [35].

下面给出反演公式(15)等的两个应用例子.

例 1 (**Reed-Muller 码的码字重量公式**). Reed-Muller (RM) 码是近代通信理论中所研究的一类重要的编码. 每个 RM 码的码字可以用 $GF(2)$ 上的 n 个变量的多项式

$$f(x_1, \cdots, x_n)=\sum a_{i_1\cdots i_n} x_1^{i_1} x_2^{i_2}\cdots x_n^{i_n} \qquad (18)$$

来表示, 其中诸系数 $a_{i_1\cdots i_n}$ 与变元 x_j 均取自, $GF(2)$, $i_p=0$ 或 1. 称 $i_1+\cdots+i_n$ 的最大值 m 为 f 的次数. 例如 $f=x_1x_2+x_2x_3+x_4+x_7$ 为二次多项式. 所有 m 次多项式 $f(x_1, \cdots, x_n)$ 的全体即构成 m 阶 RM 码. 例如二阶 RM 码即为形如 $\sum a_{ij}x_ix_j+\sum b_kx_k+c$ 的多项式之全体. 一个 RM 码的码字 $f(x_1, \cdots, x_n)$ 的重量 (记作 $|f|_n$) 定义为方程 $f(x_1, \cdots, x_n)=1$ 的不同解 $(x_1, \cdots, x_n)$ 个数. 例如对 $f(x_1, \cdots, x_5)=x_1x_2+x_3x_4$, $f=1$ 的全体解为

$$\begin{aligned}(x_1, \cdots, x_5)=&(1,1,0,0,\alpha),\ (0,0,1,1,\alpha),\\ &(1,1,0,1,\alpha),\ (0,1,1,1,\alpha),\\ &(1,1,1,0,\alpha),\ (1,0,1,1,\alpha).\end{aligned}$$

其中 $x_5=\alpha$ 可任取 0 或 1, 因此共有 12 组解, 于是 $|x_1x_2+x_3x_4|_5=12$.



定理 C. 记 F 为 $f(x_1,\cdots,x_n)$ 中单项式之全体，对 F 的任一子集 G，以 $\nu(G)$ 记在 G 中不出现的变量个数，$|G|$ 表示 G 中单项式之个数，则

$$|f|_n=\sum_{G\subseteq F,G\neq\phi}(-1)^{|G|+1}2^{|G|+\nu(G)-1}. \tag{19}$$

例如上述例子中 $f(x_1,\cdots,x_5)=x_1x_2+x_3x_4$，$F=\{x_1x_2, x_3x_4\}$，它的非空子集 G 计有

G	$\|G\|$	$\nu(G)$	$\|G\|+\nu(G)-1$
$\{x_1x_2\}$	1	3	3
$\{x_3x_4\}$	1	3	3
$\{x_1x_2, x_3x_4\}$	2	1	2

故 $|f|_5=2^3+2^3-2^2=12$.

证. 对每个 $G\subseteq F$，定义 $f(G)$ 为满足下列条件的点 $a=(a_1,\cdots,a_n)$ 的个数：G 中的每个单项式在点 a 取值为 0，而 F 中的其余单项式在点 a 取值为 1. 设在 $F\setminus G$ 中出现的变量为 $x_{i_1}, x_{i_2},\cdots,x_{i_p}$，则集合

$$M=\{(a_1,\cdots,a_n)\,|\,a_{i_1}=\cdots=a_{i_p}=1\}$$

中点 a 的个数显然等于 $2^{n-p}=2^{\nu(F\setminus G)}$. 任取 M 的一个点，则或者在 G 中可以找到一个单项式，它在 a 点取值为 0，此种点的个数易见为 $\sum\limits_{H\subset G,H\neq\phi}f(H)$；或者 G 中每个单项式在 a 点取值均为 1，此种点 a 的个数显然为 $2^{\nu(F)}=f(\phi)$. 因此

$$\sum_{H\subseteq G}f(H)=|M|=2^{\nu(F\setminus G)}.$$

应用 Möbius 反演公式(15)即得

$$f(G)=\sum_{H\subseteq G}(-1)^{|G|-|H|}2^{\nu(F\setminus H)}. \tag{20}$$

今记 $N(f)$ 为 $f(x_1,\cdots,x_n)=0$ 的根的个数，于是 $|f|_n=2^n-N(f)$，且易见



$$N(f) = \sum_{\substack{G\subseteq F\\ |F\setminus G|\equiv 0(\mathrm{mod}\,2)}} f(G).$$

将(20)式代入,并注意到 $\sum\limits_{G\subseteq F} f(G) = 2^{\nu(F\setminus F)} = 2^{\nu(\phi)} = 2^n$, 可见

$$\begin{aligned}
2N(f) &= 2^n + \sum_{G\subseteq F}(-1)^{|F|-|G|}f(G)\\
&= 2^n + \sum_{G\subseteq F}(-1)^{|F|-|G|}\sum_{H\subseteq G}(-1)^{|G|-|H|}2^{\nu(F\setminus H)}\\
&= 2^n + \sum_{H\subseteq F}(-1)^{|F|-|H|}2^{\nu(F\setminus H)}\sum_{H\subseteq G\subseteq F}1\\
&= 2^n + \sum_{H\subseteq F}(-1)^{|F|-|G|}2^{\nu(F\setminus H)}2^{|F|-|H|}\\
&= 2^n + \sum_{G\subseteq F}(-1)^{|G|}2^{\nu(G)}2^{|G|}\\
&= 2^{n+1} + \sum_{G\subseteq F,G\neq\phi}(-1)^{|G|}2^{\nu(G)+|G|}.
\end{aligned}$$

此即 $N(f) = 2^n + \sum\limits_{G\subseteq F,G\neq\phi}(-1)^{|G|}2^{\nu(G)+|G|-1}$ 或即 $|f|_n = 2^n - N(f) = \sum\limits_{G\subseteq F,G\neq\phi}(-1)^{|G|+1}2^{\nu(G)+|G|-1}$.

公式(19)中和式包含了 $2^{|F|}$ 个加项,故当 F 项数很多时,用它来计算 $|f|_n$ 并不方便,有时用其他方法计算 $|f|_n$ 更为简单. 但由(19)式我们可以推出有关 RM 码的码字的一个性质. 为此我们注意,若 $G\subset F$, G 的次数为 d, 则 $\nu(G)\geqslant n-|G|d$, 此即 $|G|\geqslant\lceil(n-\nu(G))/d\rceil$. (这里 $\lceil x\rceil$ 定义为不小于 x 的最小整数.) 从而 $\nu(G)+|G|\geqslant\nu(G)+\lceil(n-\nu(G))/d\rceil\geqslant\lceil n/d\rceil$. 但对 m 阶 RM 码, $d\leqslant m$, 故 $\nu(G)+|G|\geqslant\lceil n/m\rceil$, 于是由(19)式推出

命题 6. m 阶 RM 码的码字 $f(x_1,\cdots,x_n)$ 之重量必为 $2^{\lceil n/m\rceil-1}$ 的倍数.



例 2 （**Euler φ 函数**）. 对于正整数 n，函数 $\varphi(n)$ 定义为不超过 n 且与 n 互素的正整数个数。例如对 $n=12$，不超过 12 且与之互素的正整数有 1, 5, 7, 11，故 $\varphi(12)=4$。$\varphi(n)$ 是数论中常用的一种函数，今确定 $\varphi(n)$ 的表示式，为此将 $N=\{1, 2, \cdots, n\}$ 中各数按其与 n 的最大公因数分类，亦即记 $S_d=\{i \mid i\in N, \gcd(i, n)=d\}$. 于是 $N=\bigcup\limits_{d\mid n} S_d$，因此 $n=\sum\limits_{d\mid n}|S_d|$. 但 $i\in S_d$ 当且仅当 $i=kd$，$\gcd(k, n/d)=1$，故 $|S_d|=\varphi(n/d)$，所以 $n=\sum\limits_{d\mid n}\varphi(n/d)=\sum\limits_{d'\mid n}\varphi(d')$、应用反演公式(3.1.5)即得

$$\varphi(n)=\sum_{d\mid n}\mu(n/d)d=\sum_{d'\mid n}\mu(d')n/d'.$$

设 $n=\prod\limits_i p_i^{\alpha_i}$ 为它的因子分解式（$\alpha_i\geqslant 1$），则由 $\mu(d)$ 的表示式(3.1.6)可见

$$\begin{aligned}\varphi(n)&=n-\sum_i n/p_i+\sum_{i<j} n/p_ip_j\\&\quad-\sum_{i<j<k} n/p_ip_jp_k+\cdots\\&=n\prod_i(1-1/p_i)\\&=\prod_i p_i^{\alpha_i-1}(p_i-1).\end{aligned}\tag{21}$$

例如 $12=2^2\times 3$，故 $\varphi(12)=2\times(2-1)\times(3-1)=4$。

在文献 Bender and Goldman [35] 中列举了 Möbius 反演公式在对称函数理论、图的色数多项式、凸多面体理论、有限域上向量空间计数等多方面的应用，于此不再一一引述。



3.4. “入与出原理”及其应用

本节我们将应用 Möbius 反演公式引出组合计数方法中的一个重要原理——入与出原理，又称容斥原理。

考察一个 n 元的集合 $A=\{a_1, a_2, \cdots, a_n\}$，集合 A 中不同的元往往具有不同的性质．具体言之，设有 r 种性质 $P=\{p_1, p_2, \cdots, p_r\}$．将集合 A 中具有性质 p_i 的元之全体记作 A_i，又对 $P=\{p_1, \cdots, p_r\}$的任一子集 $T=\{p_{i_1}, p_{i_2}, \cdots, p_{i_s}\}$，用 $N_{\geqslant}(T)$ 表示集合 A 中同时具有性质 $p_{i_1}, \cdots, p_{i_s}$（可能还具有别的性质 p_j）的元的个数；以 $N_{=}(T)$ 表示 A 中恰具有性质 $p_{i_1}, \cdots, p_{i_s}$（不具有 P 中别的任一性质）的元的个数，则显见

$$N_{\geqslant}(T)=\sum_{X\supseteq T} N_{=}(X).$$

这是因为对每个同时具有性质 $p_{i_1}, \cdots, p_{i_s}$ 的元 a 必存在一个 $X\supseteq T$，使得元 a 恰具有 X 中的各个性质．应用 Möbius 反演公式(3.3.16)即得

$$N_{=}(T)=\sum_{X\supseteq T}(-1)^{|X|-|T|}N_{\geqslant}(X). \tag{1}$$

特别对于 $T=\phi$，$N_{=}(\phi)$ 即表示 A 中不具有 P 中任一性质的元的个数．于是

$$N_{=}(\phi)=\sum_{X}(-1)^{|X|}N_{\geqslant}(X), \tag{2}$$

式中和式遍及 P 的所有子集 X．这一等式可以写成更明显的形式．为此用 $n(p_{i_1}, \cdots, p_{i_k}, \bar{p}_{j_1}, \cdots, \bar{p}_{j_l})$ 表示 A 中同时具有性质 $p_{i_1}, \cdots, p_{i_k}$ 而又不具有 $\bar{p}_{j_1}, \cdots, \bar{p}_{j_l}$ 的元的个数．例如对 $X=\{p_1\}$，$N_{\geqslant}(X)$ 即 $n(p_1)$，而 $N_{=}(X)$ 即 $n(p_1, \bar{p}_2, \bar{p}_3, \cdots, \bar{p}_r)$．于是由(2)式得出



定理 A（入与出原理）.

$$n(\bar{p}_1, \bar{p}_2, \cdots, \bar{p}_r) = n - \sum_i n(p_i)$$
$$+ \sum_{i<j} n(p_i, p_j) - \sum_{i<j<k} n(p_i, p_j, p_k) + \cdots$$
$$+ (-1)^r n(p_1, p_2, \cdots, p_r). \qquad (3)$$

注意到上式与等式 $n(1-p_1)(1-p_2)\cdots(1-p_r) = n - \sum np_i + \sum np_ip_j - \sum np_ip_jp_k + \cdots$ 的相似性可以帮助我们记住这一等式.

在一般情形，例如求 $n(p_1, p_2, \bar{p}_3, \bar{p}_4)$，可在（1）式中令 $P = \{p_1, p_2, p_3, p_4\}$，$T = \{p_1, p_2\}$，即可得出

$$n(p_1, p_2, \bar{p}_3, \bar{p}_4) = n(p_1, p_2) - n(p_1, p_2, p_3)$$
$$- n(p_1, p_2, p_4) + n(p_1, p_2, p_3, p_4), \qquad (4)$$

一如等式 $np_1p_2(1-p_3)(1-p_4) = np_1p_2 - np_1p_2p_3 - np_1p_2p_4 + np_1p_2p_3p_4$.

入与出原理还可改写成其他形式. 如前所述，每一种性质 p_i 均对应一 A 中子集 A_i，从而 $n(p_i) = |A_i|$，$n(\bar{p}_i) = |A \backslash A_i| = n - |A_i|$，同样 $n(p_ip_j) = |A_i \cap A_j|$ 等等，于是(3)式可以写成

$$|\bar{A}_1 \cap \bar{A}_2 \cap \cdots \cap \bar{A}_n| = n - \sum |A_i|$$
$$+ \sum |A_i \cap A_j| - \sum |A_i \cap A_j \cap A_k| + \cdots. \qquad (5)$$

但 $|\bar{A}_1 \cap \bar{A}_2 \cap \cdots \cap \bar{A}_n| = \overline{|A_1 \cup A_2 \cup \cdots \cup A_n|} = n - |A_1 \cup A_2 \cup \cdots \cup A_n|$，故有

定理 B（入与出原理）.

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_i |A_i|$$
$$- \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \cdots$$
$$+ (-1)^n |A_1 \cap A_2 \cap \cdots \cap A_n|. \qquad (6)$$



当 $n=3$ 时即

$$|A\cup B\cup C|=|A|+|B|+|C|-|A\cap B|$$
$$-|A\cap C|-|B\cap C|+|A\cap B\cap C|. \qquad (7)$$

它表示为了计算三个集合之并 $A\cup B\cup C$ 中元的个数，我们很自然地先分别计入集合 A, B, C 的元的个数之和 $|A|+|B|+|C|$. 但这样做我们发现：两个集合的公共部分 $A\cap B$, $A\cap C$ 与 $B\cap C$ 的元被计入了两次（见图 1），故应从

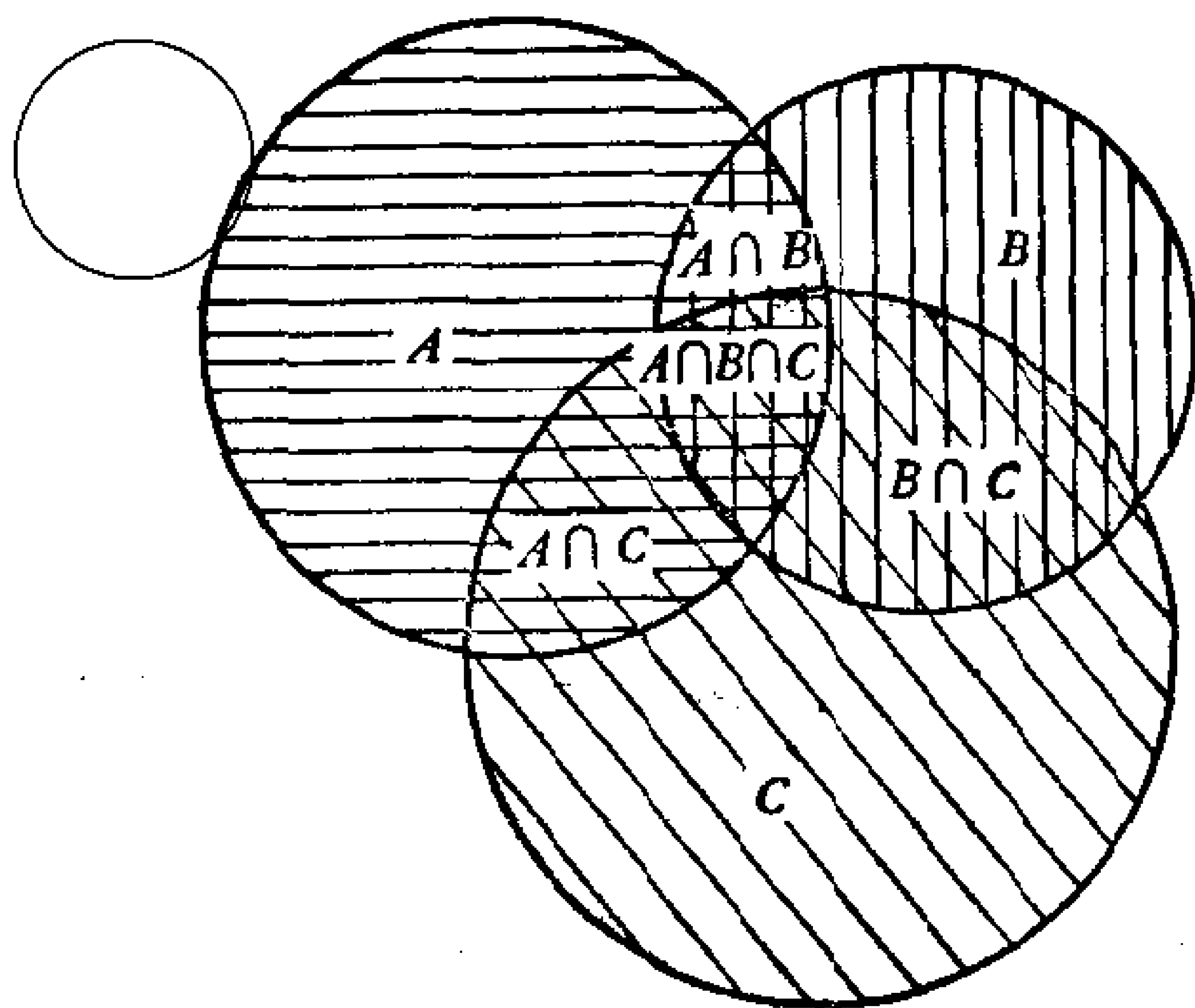


图 1.

$|A|+|B|+|C|$ 中扣出去多计入的 $|A\cap B|$ 等，得 $|A|+|B|+|C|-|A\cap B|-|A\cap C|-|B\cap C|$. 然而这样一来，三个集合的公共部分 $A\cap B\cap C$ 只计入了 0 次（在 $|A|+|B|+|C|$ 中被计入了 3 次，在 $-|A\cap B|-|A\cap C|-|B\cap C|$ 中被扣出去 3 次），故应再计入 $|A\cap B\cap C|$. (6)式即表示了这种反复"计入"与"扣出去"的过程，此即"入与出原理"名称的由来.

今对 $\{1,2,\cdots,n\}$ 的任一子集 X，记

$$f(X)=\left|\bigcup_{i\in X}A_i\right|,\quad g(X)=\left|\bigcap_{i\in X}A_i\right|,$$

则(6)式可以写成



$$f(X)=\sum_{Y\subseteq X}(-1)^{|Y|+1}g(Y).$$

再次应用 Möbius 反演公式(3.3.15),即得

$$g(X)=\sum_{Y\subseteq X}(-1)^{|Y|+1}f(Y).$$

由此引出入与出原理的第三种表示形式

定理 C (入与出原理).

$$|A_1\cap A_2\cap\cdots\cap A_n|=\sum|A_i|-\sum|A_i\cup A_j|+\sum|A_i\cup A_j\cup A_k|-\cdots. \tag{8}$$

(6)式与(8)式当 $n=2$ 时得出同一等式

$$|A\cup B|+|A\cap B|=|A|+|B|. \tag{9}$$

此式易直接证得. (6)与(8)也可由(9)式出发,用归纳法加以证明. 此时要用到运算∪与∩的分配律: $A\cap\left(\bigcup_i B_i\right)=\bigcup_i(A\cap B_i)$ 及 $A\cup\left(\bigcap_i B_i\right)=\bigcap_i(A\cup B_i)$.

入与出原理的三种形式可用于不同的计数场合,例如(8)式可用于 $\left|\bigcup_i A_i\right|$ 的计数容易,而 $\left|\bigcap_i A_i\right|$ 较难的场合, (6)式则反之.

定理 D (筛法公式). 设 $A_1, A_2, \cdots, A_r$ 为 A 的一组子集,则对固定的 $p>0$, A 中恰好属于其中 p 个子集的元的个数 $N_{r,p}$ 为

$$N_{r,p}=\sum_{k=p}^{r}(-1)^{k-p}\binom{k}{p}\sum_{\substack{I\subseteq R\\|I|=k}}\left|\bigcap_{i\in I}A_i\right|, \tag{10}$$

其中 $R=\{1,2,\cdots,r\}$.

证. 考察 R 的一个 p 元子集 P, 在(5)式中以 $\bigcap_{i\in P}A_i$ 代



A, $A_j \cap \left(\bigcap_{i\in P} A_i\right)$ 代 A_j，则得

$$\left|\bigcap_{i\in P} A_i \cap \left(\bigcap_{j\in R\setminus P} \overline{A}_j\right)\right|$$

$$= \left|\bigcap_{i\in P} A_i\right| - \sum_{\substack{K\supseteq P\\ |K|=p+1}} \left|\bigcap_{i\in K} A_i\right| + \cdots$$

$$= \sum_{K\supseteq P} (-1)^{|K|-|P|} \left|\bigcap_{i\in K} A_i\right|$$

$$= \sum_{k=p}^{r} (-1)^{k-p} \sum_{\substack{K\supseteq P\\ |K|=k}} \left|\bigcap_{i\in K} A_i\right|,$$

故

$$N_{r,p} = \sum_{|P|=p} \left|\bigcap_{i\in P} A_i \bigcap_{j\in R\setminus P} \overline{A}_j\right|$$

$$= \sum_{|P|=p} \sum_{k=p}^{r} (-1)^{k-p} \sum_{\substack{K\supseteq P\\ |K|=k}} \left|\bigcap_{i\in K} A_i\right|$$

$$= \sum_{k=p}^{r} (-1)^{k-p} \sum_{|K|=k} \sum_{\substack{|P|=p\\ K\supseteq P}} \left|\bigcap_{i\in K} A_i\right|$$

$$= \sum_{k=p}^{r} (-1)^{k-p} \binom{k}{p} \sum_{|K|=k} \left|\bigcap_{i\in K} A_i\right|.$$

入与出原理可按下列方式加以推广：设 $A=\{a_1, a_2, \cdots, a_n\}$ 为一 n-集，集中每一元 a 都赋有重量 $w(a)$，它可以是实数或更一般地为任意域中的元. 对 A 的子集 $S\subseteq A$，S 的重量 $w(S)$ 定义为 $w(S)=\sum_{a\in S} w(a)$. 当诸元 a 的重量 $w(a)$ 都等于 1 时，$w(S)$ 即等于 $|S|$. 在这种赋有重量的情形时，相仿有下列定理成立：

定理 B′. $w\left(\bigcup_{i\in R} A_i\right) = \sum_{I\subseteq R} (-1)^{|I|+1} w\left(\bigcap_{i\in I} A_i\right)$.



定理 C′. $w\left(\bigcap_{i\in R} A_i\right)=\sum_{I\subseteq R}(-1)^{|I|+1}w\left(\bigcup_{i\in I} A_i\right).$

定理 D′. 设 $A_1, \cdots, A_r$ 为 A 的一组子集，则对固定的 $p>0$，A 中恰好属于其中 p 个子集的元的重量和等于

$$W_{r,p}=\sum_{k=p}^{r}(-1)^{k-p}\binom{k}{p}\sum_{\substack{I\subseteq R\\|I|=k}}W\left(\bigcap_{i\in I}A_i\right).$$

取 $w(a)=1$ 时，上述三个定理分别化作定理 B, C, D. 上述推广形式的证明亦相仿，可以 Möbius 反演公式逐步推出，读者可作为一个练习推证之.

下面我们给出几个应用例子.

例 1 (Euler φ 函数). Euler 函数之定义见上节例 2，今应用(3)式再次导出它的表示式(3.3.21). 为此设 $n=p_1^{i_1}\cdots p_r^{i_r}$ 为 n 的素因子分解式，$p_1, \cdots, p_r$ 为互异素数. 取定理 A 中的 $A=\{1, 2, \cdots, n\}$，性质 p_i 取为"是 p_i 的倍数". A 中以 p_i 为因子的数显然有 n/p_i 个，即 $n(p_i)=n/p_i$、同样 $n(p_ip_j)=n/p_ip_j$ $(i<j), \cdots$. 一个数 k 欲与 n 互素，当且仅当它不含有任一因子 p_i，所以 $\varphi(n)=n(\bar{p}_1, \cdots, \bar{p}_r)$，于是

$$\begin{aligned}\varphi(n)&=n-\sum n/p_i+\sum n/p_ip_j-\sum n/p_ip_jp_k+\cdots\\&=n\prod_k(1-1/p_k)=\prod_k p_k^{i_k-1}(p_k-1).\end{aligned}$$

例 2 (重排问题). 用 $\pi=(\pi(1), \cdots, \pi(m))$ 表示 m 个文字 $1, 2, \cdots, m$ 的一个排列. 重排问题(见 3.1 节)乃要求计算出满足条件 $\pi(i)\neq i$ 的排列个数. 为应用定理 A，我们以性质 p_i 表示排列 π 满足 $\pi(i)=i$. 此种排列除去要求 $\pi(i)=i$ 外，对其余 $\pi(j)$ 别无要求，故有 $(m-1)!$ 种取法，此即 $n(p_i)=(m-1)!$ 同样 $n(p_i, p_j)=(m-2)!$，$n(p_i, p_j, p_k)=(m-3)!$ 等等. 故



$$D_n = m! - \sum_{i} (m-1)! + \sum_{i<j} (m-2)! - \cdots$$

$$= m! - \binom{m}{1}(m-1)! + \binom{m}{2}(m-2)! - \cdots$$

$$= m!(1 - 1/1! + 1/2! - 1/3! + \cdots + (-1)^m/m!).$$

例 3 (对子问题). 求满足条件 $\pi(i) \neq i$ 和 $i+1$ ($i=1, 2, \cdots, m-1$) 及 $\pi(m) \neq m$ 和 1 的 m-排列个数 $T(m)$.

仿照例 2, 以性质 p_{2i-1} ($i=1, 2, \cdots, m$) 表示 $\pi(i)=i$; 又以性质 p_{2i} ($i=1, \cdots, m-1$) 表示 $\pi(i)=i+1$, p_{2m} 表示 $\pi(m)=1$. 此时 $A_{2i-1}=\{\pi|\pi(i)=i\}$, $A_{2i}=\{\pi|\pi(i)=i+1\}$ ($i \leqslant m-1$) 及 $A_{2m}=\{\pi|\pi(m)=1\}$. 应用定理 A, 取其中的集合 A 为 $m!$ 个排列的全体, 于是 $n=|A|=m!$.

$$T(m) = n(\bar{p}_1, \bar{p}_2, \cdots, \bar{p}_{2m})$$
$$= m! - \sum|A_i| + \sum|A_i \cap A_j| - \cdots,$$

由排列的定义显见 $A_{2i-1} \cap A_{2i} = \phi$ ($i=1, 2, \cdots, m$), $A_{2i} \cap A_{2i+1} = \varnothing$ ($i=1, 2, \cdots, m-1$) 及 $A_{2m} \cap A_1 = \varnothing$. 因此对 $\{1、2, \cdots, 2m\}$ 的 k-子集 K, 若 K 中包含了序列 $(1, 2, \cdots, 2m, 1)$ 中相继的二个数, 则 $\left|\bigcap_{i \in K} A_i\right| = 0$; 而当 K 中不包含序列 $(1, 2, \cdots, 2m, 1)$ 的相继两个数时, $\bigcap_{i \in K} A_i$ 中的任一排列 π, 诸值 $\pi(i)$ ($i=1, 2, \cdots, m$) 中有 k 个值已经确定, 剩下 $m-k$ 个值有 $(m-k)!$ 种确定的方式, 因此此时 $\left|\bigcap_{i \in K} A_i\right| = (m-k)!$. 所以

$$T(m) = m! - f^*(2m, 1)(m-1)!$$
$$+ f^*(2m, 2)(m-2)! - \cdots,$$



其中 $f^*(2m, k)$ 表示集 $\{1, 2, \cdots, 2m\}$ 中不包含序列$(1, 2, \cdots, 2m, 1)$ 的相邻二元的 k-子集个数，此种元的个数等于(见(2.1.4) 式) $f^*(2m, k) = (2m/2m-k)\binom{2m-k}{k}$，故

$$T(m) = \sum_{k=0}^{m} (-1)^k (2m/2m-k) \times \binom{2m-k}{k} (m-k)!. \tag{11}$$

这一问题也可改述成下列形式：设有 $2m$ 个座位排成圆环状，另有 m 个对子 $(a_1, b_1), \cdots, (a_m, b_m)$. 今首先将 $a_1, \cdots, a_m$ 依次放到座位 $1, 3, 5, \cdots, 2m-1$ 上，然后将 b_i 放到偶数号座位上，但要求 a_i 与 b_i 不相邻 $(i = 1, \cdots, m)$，问有多少种排法？此即"对子问题"称呼的由来.

例 4. 考察无向图 G，它的顶点集合记作 V. 若 V 中两点在 G 中有边相连，则称此两点相邻. 顶点 x 的次数 $d(x)$ 定义为与 x 相邻的点的个数. 一个 r 个点的无向图 K，若 K 中诸点两两相邻，则称 K 为 r 个点的完全图，一般记作 K_r. 如图 2 所示的 K_5. 显然，若一个图中与每一点相邻的点数都相

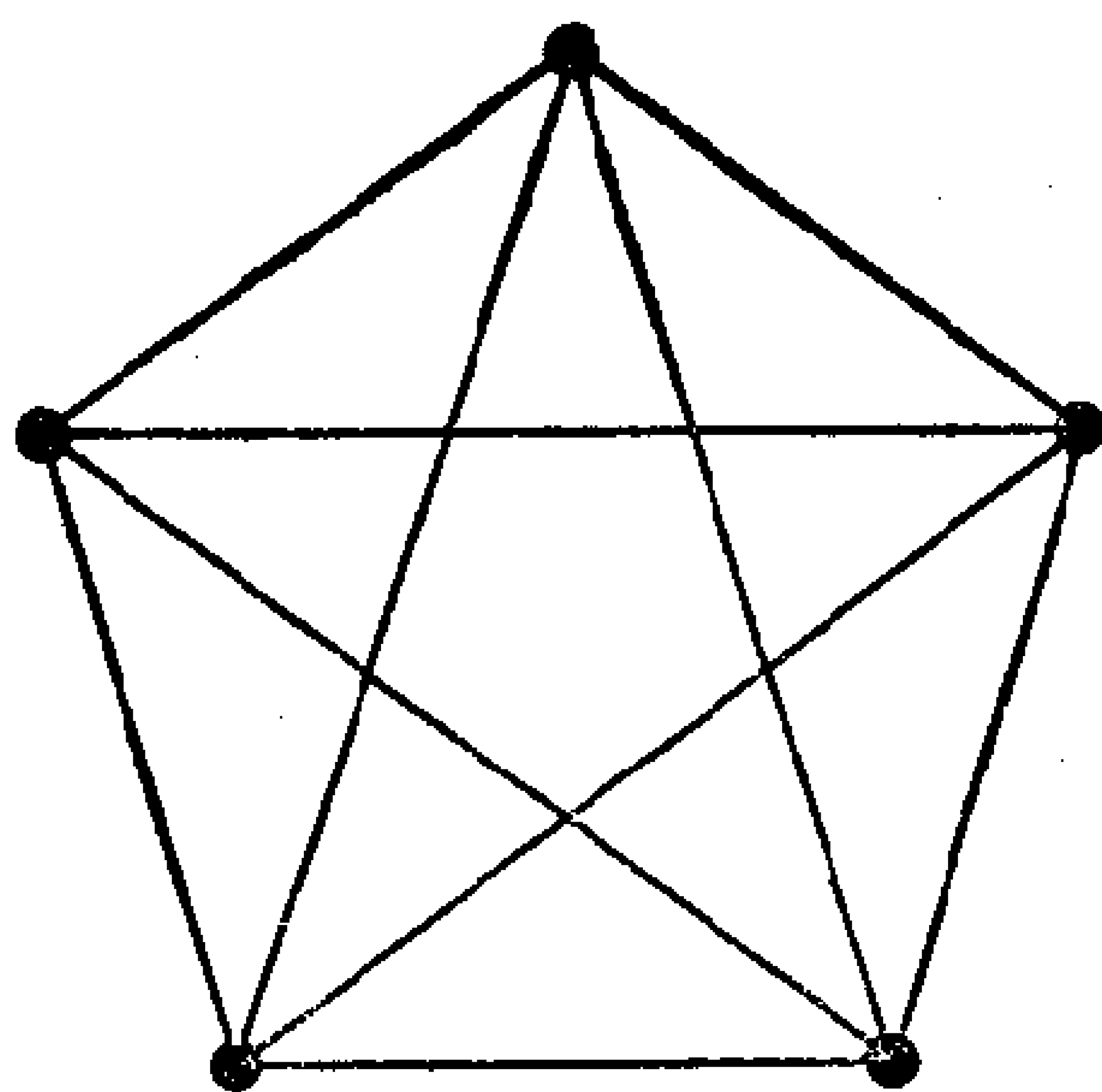


图 2.



当多时，就有可能找到该图的一个完全子图来，下面的定理给出了这方面的一个估计式.

定理 E. 若对图 G 的每个顶点 x 均有

$$d(x) \geqslant [(s-2)n/(s-1)]+1,$$

其中 n 为 G 中顶点的个数，则 G 有完全子图 K_s.

证. 设 $(s-2)n=p(s-1)+r,\ 0\leqslant r\leqslant s-2$. 又对 $x\in V$，以 $A(x)$ 表示 x 的所有邻点构成的集合. 于是按照假设，对每一 $x\in V$ 均有 $|A(x)|=d(x)\geqslant p+1$. 今按下列方式选出 V 中的一个点列 $x_1, x_2, \cdots, x_q$. 其中初始点在 V 中任意选取，x_1 选定后，任取 $x_2\in A(x_2)$，再取 $x_3\in A(x_1)\cap A(x_2), \cdots$，一般 $x_1, \cdots, x_l$ 选定后，只要 $\bigcap\limits_{i=1}^{l} A(x_i)$ 非空，则从中任选一点作为 x_{l+1}，如此反复直至 $\bigcap\limits_{i=1}^{q} A(x_i)=\phi$ 时终止. 现证此点列的个数 $q\geqslant s$，亦即当 $l<s$ 时，$\bigcap\limits_{i=1}^{l} A(x_i)$ 非空，为此记 $N_l=\left|\bigcap\limits_{i=1}^{l} A(x_i)\right|$，我们用归纳法证明

$$N_l\geqslant l(p+1)-(l-1)n. \tag{12}$$

当 $l=1$，由假设知此式为真. 今归纳假设 $N_{l-1}\geqslant(l-1)(p+1)-(l-2)n$，于是由 (9) 式并注意到对 V 的任一子集 S 必有 $|S|\leqslant|V|=n$，可得

$$N_l=\left|\bigcap_{i=1}^{l} A(x_i)\right|=\left|A(x_l)\cap\left(\bigcap_{i=1}^{l-1} A(x_i)\right)\right|$$

$$=|A(x_l)|+\left|\bigcap_{i=1}^{l-1} A(x_i)\right|$$



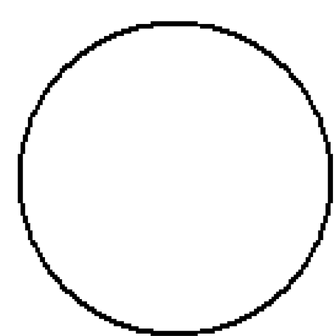
$$- \left| A(x_l) \cup \left(\bigcap_{i=1}^{l-1} A(x_i) \right) \right|$$
$$\geqslant (p+1) + (l-1)(p+1)$$
$$- (l-2)n - n = l(p+1) - (l-1)n.$$

(12)式归纳证毕. 令 $l = s-1$, 即得

$$\left| \bigcap_{i=1}^{s-1} A(x_i) \right| \geqslant (s-1)(p+1) - (s-2)n$$
$$= (s-1)(p+1) - (p(s-1)+r)$$
$$= (s-1) - r \geqslant 1.$$

此即表明所选取的点列 $x_1, \cdots, x_q$ 之长 $q \geqslant s$. 而此一点列由作法可见两两相邻,故G有完全子图 $K_q \supseteq K_s$.

3.5. 矩阵的常值



对于一个m行, n列的矩阵 $A=(a_{ij})$ $(m \leqslant n)$, A的常值 Per(A) 定义为

$$\mathrm{Per}(A) = \sum_{\pi} a_{1\pi(1)} a_{2\pi(2)} \cdots a_{m\pi(m)}. \tag{1}$$

其中和式遍及 $\{1, 2, \cdots, n\}$ 的所有 m-排列. 特别当 $m=n$, 即A为n阶方阵时, (1) 中的和式遍及$\{1, 2, \cdots, n\}$的$n!$ 个排列, 此时 Per(A) 与通常的行列式 det(A) 之定义相比,其区别仅在(1)中各加项前均冠以正号. 一些组合问题的解常可表示成 Per(A) 的形式,其中A为(0,1)矩阵. 例如为了求出满足 $\pi(i) \neq i$ $(i=1, \cdots, n)$ 的排列π的个数 (重排问题) D_n, 我们可令 $a_{ii}=0$, $a_{ij}=1$ $(i \neq j)$, 则 Per(A) 即为解数 D_n. 此因和式(1)中, 加项 $\prod_i a_{i\pi(i)}=1$ 当且仅当 $a_{1\pi(1)} = a_{2\pi(2)} = \cdots = a_{n\pi(n)} = 1$, 亦即当且仅当排列$\pi$满足



$\pi(i) \neq i$ $(i=1, 2, \cdots, n)$. 同样为了求出对子问题的解（见 3.4 节），可令 $a_{ii}=a_{ii+1}=0$ $(i=1, \cdots, n-1)$, $a_{n1}=a_{nn}=0$, 则 $T(n)=\mathrm{Per}(A)$. 一般为了求出一类带限制 $\pi(i) \notin A(i) \subseteq \{1, 2, \cdots, n\}$ $(i=1, 2, \cdots, n)$ 之排列个数，我们可令

$$a_{ij}=\begin{cases}0, & 若\ j \in A_i; \\ 1, & 其他情形.\end{cases}$$

则 $\mathrm{Per}(A)$ 即为所求的解数. (0, 1) 矩阵 A 的常值还可用来表出一组子集的"互异表示系"的个数：设 $S_1, S_2, \cdots, S_m$ 是集合 S 的一组子集，若可选出 m 个互不相同的元 $a_1, \cdots, a_m$，使得 $a_i \in S_i$ $(i=1, \cdots, m)$，则称 $a_1, \cdots, a_m$ 构成子集系 $S_1, \cdots, S_m$ 的一组"互异表示系". "互异表示系"是构造性组合数学中所研究的一个重要对象，它在拉丁方理论等方面均有应用. 设 $S=\{a_1, \cdots, a_n\}$, $S_1, S_2, \cdots, S_m$ 为 S 的一组子集. 为了计算该组子集的各互异表示系个数，我们可令

$$a_{ij}=\begin{cases}1, & 若\ a_j \in S_i; \\ 0, & 其他情形.\end{cases}$$

则 $\mathrm{Per}(A)$ 即为欲求的组数. 此因和式(1)中 $\Pi a_{i\pi(i)}=1$ 当且仅当 $a_{1\pi(1)}=\cdots=a_{m\pi(m)}=1$，此即 $a_{\pi(1)} \in S_1, \cdots, a_{\pi(m)} \in S_m$，而 $\pi(1), \cdots, \pi(m)$ 既然为一 m-排列，当有 $\pi(i) \neq \pi(j)$ $(i \neq j)$，由此可见诸元 $a_{\pi(i)}$ 互异，所以 (1) 中每一非零项 1 都相应于 $S_1, \cdots, S_m$ 的一组互异表示系.

对于 n 阶方阵，由 $\mathrm{Per}(A)$ 与 $\det(A)$ 定义的相似性可以推知，行列式的某些性质也适用于 $\mathrm{Per}(A)$. 例如：$\mathrm{Per}(A^T)=\mathrm{Per}(A)$ （A^T 表示阵 A 的转置）；又如 Laplace 展开定理；另外，对任意的置换矩阵 P 与 Q, $\mathrm{Per}(PAQ)=\mathrm{Per}(A)$ 成立，亦即改变 A 中行与列的次序，不影响其常值. 这些简单性质，有时可用于 $\mathrm{Per}(A)$ 之计算. 例如对行列式的特征多项



式，有

$$\det(A-\lambda I)=\sum_{k=0}^{n}(-\lambda)^{n-k}S_k,$$

其中 S_k 为 A 的所有 k 阶主子式之和．对于常值，相仿有

$$\operatorname{Per}(A-\lambda I)=\sum_{k=0}^{n}(-\lambda)^{n-k}S_k, \tag{2}$$

其中

$$S_k=\sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n}\operatorname{Per}\begin{pmatrix}i_1 i_2\cdots i_k\\ i_1 i_2\cdots i_k\end{pmatrix},$$

其中 $\begin{pmatrix}i_1\cdots i_k\\ j_1\cdots j_k\end{pmatrix}$ 表示由 A 中第 $i_1,\cdots,i_k$ 行，$j_1,\cdots,j_k$ 列形成的子阵．应用(2)式于重排问题

$$D_n=\operatorname{Per}(J-I),$$

其中 $J=J_n$ 为 n 阶方阵，它的元都等于 1，而 I 为 n 阶单位矩阵，即得

$$\operatorname{Per}(J-\lambda I)=\sum_{k=0}^{n}(-\lambda)^{n-k}\binom{n}{k}k!$$

$$=\sum_{k=0}^{n}(-\lambda)^{n-k}n!/(n-k)!.$$

因此时对于 J_k 而言显然有 $\operatorname{Per}(J_k)=k!$．在上式中令 $\lambda=1$，即得

$$D_n=\operatorname{Per}(J-I)=n!\sum_{k=0}^{n}(-1)^k/k!.$$

然而，行列式的一个最重要的性质："将一行乘以常数后加到另一行上，其值不变"，对于 $\operatorname{Per}(A)$ 却不成立．这就使得 $\operatorname{Per}(A)$ 的计算在大多数场合十分困难．在计算机上，若直接从 $\operatorname{Per}(A)$ 的定义出发进行计算，则约需 $n\cdot n!$ 次算术运算，其中还未计入为了顺序生成 $n!$ 个排列所需的运算．在



Nijenhuis [118] 中提出了一种运算次数大为减少的算法，它的出发点是 Ryser 所发现的下面的定理:

定理 A. 设 A 为 n 阶方阵, A_r 为从矩阵 A 中将某 r 列易为 0 得出的矩阵. 以 $S(A_r)$ 表示矩阵 A_r 的各行元之和的乘积,又以 $\sum S(A_r)$ 表示对各种可能的 A_r 求和,则

$$\begin{aligned}\operatorname{Per}(A) = \sum S(A_{n-m}) - \binom{n-m+1}{1} \sum S(A_{n-m+1}) \\ + \binom{n-m+2}{2} S(A_{n-m+2}) - \cdots \\ + (-1)^{m-1} \binom{n-1}{m-1} \sum S(A_{n-1}).\end{aligned} \tag{3}$$

尤取 $m = n$, 对 n 阵方阵 A 便有

$$\begin{aligned}\operatorname{Per}(A) = S(A) - \sum S(A_1) \\ + \sum S(A_2) - \cdots + (-1)^{n-1} S(A_{n-1}).\end{aligned} \tag{4}$$

例如,对

$$A = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix},$$

$$A_1 = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix},$$

$$\begin{aligned}\operatorname{Per}(A) &= S(A) - \sum S(A_1) + \sum S(A_2) \\ &= 2^3 - (2 + 2 + 2) + 0 = 2.\end{aligned}$$

证. 取 S 为数字 $1, 2, \cdots, n$ 的所有 m-排列 $\sigma = (j_1, \cdots, j_m)$ 之全体, 对每个 $\sigma \in S$ 赋予重量 $w(\sigma) = a_{1j_1} a_{2j_2} \cdots$



a_{mj_m}. 又若诸 $j_k \neq i$ $(k=1,\cdots,m)$ 时称 σ 具有性质 $P_i(i=1,\cdots,n)$. 今设 A_r 为在 A 中令第 $i_1, i_2, \cdots, i_r$ 列为 0 得来的阵,则易见

$$w(P_{i_1}, P_{i_2}, \cdots, P_{i_r}) = S(A_r).$$

这里 $w(P_{i_1}, \cdots, P_{i_r})$ 表示 S 中具有性质 $P_{i_1}, \cdots, P_{i_r}$ 的元之重量和,因此若以 $w(r)$ 记 S 中恰具有 r 个性质 p_i 的元 σ 之重量和,则

$$w(r) = \sum S(A_r).$$

今 Per(A) 按定义应等于 S 中恰具有 $n-m$ 个性质 P_i 的元之重量和,故由上节定理 D' 即得证本定理.

计算 Per(A) 的另一种方法是应用次之通称为 **"MacMahon 主定理"**的公式.

定理 B.

$$\mathrm{Per}(A) = C(x_1x_2\cdots x_n):(\det(I - XA))^{-1}. \tag{5}$$

其中记号 "$C(x_1x_2\cdots x_n):f(x)$" 表示 $f(x)$ 中 $x_1x_2\cdots x_n$ 项前的系数, I 为单位阵, $X=(x_i\delta_{ij})$.

(5)式可推广成更一般形式,为此引入

定义 1.

$$\mathrm{Per}^{(s_1,\cdots,s_n)}(A) \equiv C(x_1^{s_1}x_2^{s_2}\cdots x_n^{s_n}):\left(\sum_j a_{1j}x_j\right)^{s_1} \times \left(\sum_j a_{2j}x_j\right)^{s_2}\cdots\left(\sum_j a_{nj}x_j\right)^{s_n}.$$

定理 B′.

$$\mathrm{Per}^{(s_1,\cdots,s_n)}(A) = C(x_1^{s_1}x_2^{s_2}\cdots x_n^{s_n}):(\det(I - XA))^{-1}.$$

当 $s_1 = s_2 = \cdots = s_n = 1$ 时,定理 B' 即化作定理 B. 定理 B' 之证明及其在常值计算中的应用可见 Percus [126]. 下面仅举一例说明 MacMahon 主定理之应用.

命题 1 (Dixon 公式).



$$\sum_{s=0}^{2m}(-1)^s\binom{2m}{s}^3=(-1)^m(3m)!/(m!)^3. \qquad (6)$$

证. 考察积

$$(y-z)^{2m}(z-x)^{2m}(x-y)^{2m}$$

$$=\left(\sum_{s_1}(-1)^{s_1}\binom{2m}{s_1}y^{2m-s_1}z^{s_1}\right)$$

$$\times\left(\sum_{s_2}(-1)^{s_2}\binom{2m}{s_2}z^{2m-s_2}x^{s_2}\right)$$

$$\times\left(\sum_{s_3}(-1)^{s_3}\binom{2m}{s_3}x^{2m-s_3}y^{s_3}\right)$$

$$=x^{2m}y^{2m}z^{2m}\sum_{s_1,s_2,s_3}(-1)^{s_1+s_2+s_3}$$

$$\times\binom{2m}{s_1}\binom{2m}{s_2}\binom{2m}{s_3}x^{s_2-s_3}y^{s_3-s_1}z^{s_1-s_2},$$

故

$$\sum_{s=0}^{2m}(-1)^s\binom{2m}{s}^3=C(x^{2m}y^{2m}z^{2m}):$$

$$(y-z)^{2m}(z-x)^{2m}(x-y)^{2m}.$$

应用 MacMahon 主定理即见上式右边等于

$$C(x^{2m}y^{2m}z^{2m}):(\det B)^{-1}.$$

其中

$$B=\begin{pmatrix}1&&\\&1&\\&&1\end{pmatrix}-\begin{pmatrix}x&&\\&y&\\&&z\end{pmatrix}\begin{pmatrix}0&1&-1\\-1&0&1\\1&-1&0\end{pmatrix}$$

$$=\begin{pmatrix}1&x&-x\\-y&1&y\\z&-z&1\end{pmatrix}.$$

于是



$$(\det B)^{-1} = (1 + xy + yz + zx)^{-1}$$

$$= \sum_n (-1)^n (xy + yz + xz)^n$$

$$= \sum_n (-1)^n \sum_{n_1+n_2+n_3=n}$$

$$\times \binom{n}{n_1, n_2, n_3} x^{n_1+n_3} y^{n_2+n_1} z^{n_3+n_2}.$$

注意 $n_1 + n_3 = n_2 + n_1 = n_3 + n_2 = 2m$ 当且仅当 $n_1 = n_2 = n_3 = m$, 可见

$$C(x^{2m}y^{2m}z^{2m}):\ (\det B)^{-1} = (-1)^{3m} \binom{3m}{m, m, m}$$

$$= (-1)^m (3m)!/(m!)^3.$$

命题得证.

MacMahon 曾利用定理 B' 为工具,应用类似的推理, 得出了一系列其他恒等式.

关于矩阵的常值,尽管有定理 A, B 所提供的两种方法,但其计算依然十分繁复, 这就使得很多关于常值的问题迄今未能完全解决. (如见 Marcus and Minc [110].) 1926 年 van der Waerden 曾提出一个著名的猜测: 设 A 为 n 阶双随机矩阵(即 A 的元非负,每行及每列的元之和都等于 1),则

$$\operatorname{Per}(A) \geqslant n!/n^n. \tag{7}$$

这一猜测迄今未能得到完全的证明. 这一猜测在 (0, 1) 矩阵情形尤为引人注目: 若以 $U(n, k)$ 记所有每行每列有 k 个 1 的 n 阶(0, 1)阵之全体,因对 $A \in U(n, k)$, $(1/k)A$ 显然为双随机阵,由 $\operatorname{Per}(A/k) = (\operatorname{Per}(A))/k^n$, 可见猜测(7)在 (0, 1) 阵 $A \in U(n, k)$ 情形化作

猜测. $\operatorname{Per}(A) \geqslant (k/n)^n n!,\ A \in U(n, k).$ (8)

关于 $\operatorname{Per}(A)$ 的上界, 1963 年 Minc 猜测: 若 A 为 n 阶 (0,



1)阵，其各行元之和分别为 $r_1, r_2, \cdots, r_n$，则

$$\operatorname{Per}(A) \leqslant \prod_{i=1}^{n} (r_i!)^{1/r_i}. \tag{9}$$

这一猜测已为 Bregman[39] 所证明。猜测(8)与上界(9)与**拉丁方**计数问题有密切的联系：一个 $m \times n(m \leqslant n)$ 的矩阵 A，如果每一行为 $1, 2, \cdots, n$ 的一个排列，且每一列中元互异，则称为m行的拉丁矩阵。拉丁方理论在近代实验设计中有重要的应用。一个 $m \times n$ 拉丁矩阵 A，只要 $m < n$，总可增添第 $m+1$ 行使之成为$(m+1) \times n$ 拉丁矩阵。事实上，若以 S_i 记 A 中第 i 列出现的数，则任一排列 $\pi = (\pi(1), \cdots, \pi(n))$只要 $\pi(i) \notin S_i$ 都可取为第 $m+1$ 行，这种排列的个数即为带限制 $\pi(i) \notin S_i$ $(i = 1, 2, \cdots, n)$ 的排列计数问题。有如前述，这一个数可表为某个 $(0, 1)$ 阵B的常值且易见此 $B \in U(n, n-m)$，从而可证其常值必非零。因此上述拉丁矩阵的扩充总是可能的。进而若应用上界(9)，可见一个m行的拉丁矩阵至多有$((n-m)!)^{n/n-m}$ 种方式扩充成 $m+1$ 行拉丁矩阵；而若猜测(8)为真，则这种扩充方式就至少有$((n-m)^n/n^n)n!$ 种。因此若(8)式得证，便可证明 n 阶拉丁方的个数 L_n 满足不等式

$$\left(\prod_{\nu=1}^{n-1} (\nu!)^{1/\nu}\right)^n \geqslant L_n \geqslant (n!)^{2n-1}/n^{n^2}. \tag{10}$$

其中下界较之迄今已知的下界 $L_n \geqslant n!(n-1)!(n-2)!\cdots 1!$ 好得多。关于拉丁阵的计数问题，我们将在 4.4 节中继续讨论。



第四章　渐 近 计 数

4.1. 概　　述

在组合计数方法的应用中，我们常需寻求某个计数问题的解 $N(n)$ 当 n 趋于无穷时的渐近性状，这是因为通常 $N(n)$ 的表示式十分复杂，而渐近式则扬弃了和式的次要部分，突出了它的主要部分，它使我们能更清楚地了解支配这一表式的决定性部分，从而对它有更好的了解．举例来说，在计算机算法分析中，我们通常并不满足于求出一类算法的运算次数 $N(n)$ 的明显表示式，而需进一步求出，当 n 充分大时，$N(n)$ 是按线性方式 cn 增长，还是按 cn^2 方式或 $n\log n$ 等其它方式？在比较同一问题的两种算法时，使用渐近式则是很必要的．例如当 n 充分大时，算法 A 约需 $cn^{3/2}$ 次运算，而算法 B 只需要 $cn\log n$ 次运算，则算法 B 一般优于算法 A．寻求计数问题解之渐近值还有另一种原因：有很多计数问题要求出它的解的精确表示式十分困难或者根本不可能，在这种场合，我们往往设法求出它的渐近值．例如拉丁阵的计数问题（4.4节）；素数分布问题：求出不超过 x 的素数个数 $\pi(x)$ 等．要求出 $\pi(x)$ 的精确表示式是不可能的，然而著名的素数定理则指出：当 x 充分大时，$\pi(x)$ 接近于 $x/\log x$，这一渐近式深刻地反映了素数的分布规律．

与组合计数的其他方法相比，渐近计数方法需要借助于较多的分析学工具，特别是复变函数论方法．此外，渐近计数方法目前远不够完善，是一个尚有许多工作要做的领域．



下面我们引进有关渐近分析的记号和概念.

定义 1. 设 $f(n)$ 与 $g(n)$ 为正整数 n 的实值函数，则记号

$f(n)=O(g(n))$ 表示存在与 n 无关的常数 a 与 M 使得当 $a<n<+\infty$ 时 $f(n)\leqslant M|g(n)|$ 成立；

$f(n)=o(g(n))$ 表示 $\lim\limits_{n} f(n)/g(n)=0$.

特别我们常用 $O(1)$ 表示一个有界的量，而用 $o(1)$ 表示一个趋于零的量. 另外我们用

$f(n)\sim g(n)$ 表示 $f(n)=g(n)(1+o(1))$，亦即

$$\lim f(n)/g(n)=1.$$

例. 由命题 (2.5.8), $1^2+2^2+\cdots+n^2=n(n+1)\cdot(2n+1)/6=(n^3/3)+(n^2/2)+(n/6)$, 故

$$\sum_{k=1}^{n} k^2=O(n^3),\ \sum_{k=1}^{n} k^2\sim n^3/3$$

及

$$\sum_{k=1}^{n} k^2=(1/3)n^3(1+o(1)).$$

又如 $(\log n)^k=O(n)$, $e^{1/n}=1+(1/n)+o(1/n)$ 等等. 在和式变换中应用 O 记号可以使我们有效地把注意力集中于算式中的决定性部分，而不用计较一些无关紧要的细节.

关于 O 记号，我们须注意的是：1. 定义 1 中出现的常数 M 通常称为包含在 O 中的常数，这一常数在等式变换的不同阶段可以取不同的值，例如 $\sum\limits_{1}^{n} k^2=(1/3)n^3+O(n^2)=O(n^3)$，包含在前一个 O 中的常数可取作 $(1/2)+\varepsilon$ (ε 为任意正数)；而包含在后一个 O 中的常数则可取作 $(1/3)+\varepsilon$; 2. $f(n)=O(g(n))$ (或 $f(n)=o(g(n))$) 是一个单向等式，



绝不能写作 $O(g(n)) = f(n)$，不然我们就会从 $n^2/4 = O(n^2) = n^2/3$ 中引出 $n^2/4 = n^2/3$ 的荒谬结果来．一般 $O(g(n))$所表示的是"一类"函数，即与 $g(n)$ 之比为有界的一类函数之全体，故 $f(n) = O(g(n))$ 乃是表明 $f(n)$ 为函数类 $O(g(n))$ 中的一员．因而这里的"$=$"更接近于集合论中的记号"$\in$"而与寻常使用的"$=$"意义不同，之所以沿用等号，只是一个习惯的用法而已．一般我们约定等式右边所包含的函数类比等式左边更为广泛，或者说等式右边所给出的渐近式较之左边更为粗糙．因而我们可以写出 $O(n) = O(n^2)$ 而却不能写出 $O(n^2) = O(n)$.

由定义不难列出 O 记号的一些简单等式：

$$f(n) = O(f(n)),$$

$$cO(f(n)) = O(f(n)) \quad (c \text{ 为与 } n \text{ 无关的常数}),$$

$$O(f(n)) + O(g(n)) = O(f(n) + g(n)),$$

$$O(O(f(n))) = O(f(n)),$$

$$O(f(n))O(g(n)) = O(f(n)g(n)),$$

$$O(f(n)g(n)) = f(n)O(g(n)),$$

$$f(n) = O(g(n)),\ g(n) = O(h(n)) \Rightarrow f(n) = O(h(n)).$$

上述诸式除去 $f(n) = O(f(n))$ 外，对于 o 记法同样成立．此外尚成立

$$O(f(n))o(g(n)) = o(f(n)g(n)),$$

$$(o(f(n)) + o(g(n)))^k = o(f(n)^k) + o(g(n)^k),$$

$$(1 + o(f(n)))(1 + o(g(n))) = 1 + o(f(n) + g(n)),$$

$$f(n) \sim g(n),\ g(n) \sim h(n) \Rightarrow f(n) \sim h(n),$$

等等．O 记号还常用于一般实值变量 x 的函数，此时须指明 x 的变动范围．例如



$$g(x) = O(f(x)) \qquad (a \leqslant x \leqslant b)$$

表示存在常数M使得

$$|g(x)| \leqslant M\,|f(x)| \qquad (a \leqslant x \leqslant b);$$

又如

$$\sin x = O(x) \qquad (-\infty < x < +\infty),$$

$$x^2 = O(x) \qquad (-1 \leqslant x \leqslant 1),$$

等等。对于幂级数

$$g(x) = \sum a_i x^i,$$

若存在 $r > 0$，使得 $\sum |a_i| r^i < +\infty$，亦即 $\sum a_i x^i$ 在 $|x| \leqslant r$ 时绝对收敛，则常可写出

$$g(x) = a_0 + a_1 x + \cdots + a_m x^m + O(x^{m+1})$$
$$(|x| \leqslant r).$$

此因 $g(x) = a_0 + a_1 x + \cdots + a_m x^m + x^{m+1}(a_{m+1} + a_{m+2}x + \cdots)$，而当 $|x| \leqslant r$ 时，括号中的量不超过 $\sum\limits_{i=1}^{\infty} |a_{m+i}| r^{i-1} < M$.

例如对任何固定的 r，

$$e^x = 1 + x + (x^2/2!) + \cdots + (x^m/m!) + O(x^{m+1}) \qquad (|x| \leqslant r). \tag{1}$$

又当 $r < 1$ 时，

$$\log(1+x) = x - x^2/2 + \cdots + (-1)^{m+1}x^m/m + O(x^{m+1}) \qquad (|x| \leqslant r). \tag{2}$$

又如应用 $(1-x)^{-1} = \sum\limits_{i=1}^{m} x^i + O(x^{m+1})$ $(|x| < 1)$，可以得出

$$(1-\delta)^{-1} = 1 - \delta + \delta^2 + O(\delta^3) \tag{3}$$

等，其中 $\delta = o(1)$. 应用(1)与(2)又可见

$$e^\delta = 1 + \delta + (\delta^2/2) + O(\delta^3), \tag{4}$$



$$\log(1+\delta)=\delta-(\delta^2/2)+O(\delta^3). \tag{5}$$

(4),(5)两式在渐近分析中经常用到,借助于此两式可以求出某些幂次式的渐近式,如

命题 1. 设 $\alpha,\beta=O(1)$,则

$$(n+\alpha)^{n+\beta}=n^{n+\beta}e^{\alpha}(1+\alpha(\beta-\alpha/2)(1/n)+O(n^{-2})). \tag{6}$$

证. 将上式左边记作 $f(n)$,于是

$$\log f(n)=(n+\beta)\log(n+\alpha)$$
$$=(n+\beta)(\log n+\log(1+\alpha/n)),$$

应用(5)式即得

$$\log f(n)=(n+\beta)\log n+(n+\beta)(\alpha/n-\alpha^2/2n^2+O(\alpha^3/n^3))$$
$$=(n+\beta)\log n+\alpha+\alpha(\beta-\alpha/2)/n+O(n^{-2}).$$

因此

$$f(n)=n^{n+\beta}\exp(\alpha+\alpha(\beta-\alpha/2)(1/n)+O(n^{-2})). \tag{7}$$

再由(4)式得

$$(n+\alpha)^{n+\beta}=n^{n+\beta}e^{\alpha}(1+\alpha(\beta-\alpha/2)(1/n)+O(n^{-2})).$$

注意,由(7)式两边除以 $n^{n+\beta}$ 可得

$$(1+\alpha/n)^{n+\beta}=\exp(\alpha+\alpha(\beta-\alpha/2)(1/n)+O(n^{-2})). \tag{8}$$

用同样方法可以证明与此相仿的

命题 2. 若 $\alpha=o(n)$,则

$$(1+\alpha/n)^{n+\alpha}=\exp(\alpha+\alpha^2/2n+O(\alpha^3/n^2)), \tag{9}$$

$$(1+\alpha/n)^{n}=\exp(\alpha-\alpha^2/2n+O(\alpha^3/n^2)). \tag{10}$$

在运用 O 记号估计和式时,还常常涉及到"一致性"问题。



设若我们要估计和式 $\sum_{k\in S} a_k(n)$，此处 S 为一类数集，可以与 n 有关，例如 $S=\{1,2,\cdots,n\}$. 若对任意固定的 k，有 $a_k(n)=O(b_k(n))$，则并不能由此马上推出 $\sum_k a_k(n) = O\left(\sum_k b_k(n)\right)$，这是因为隐含在 $a_k(n)=O(b_k(n))$ 中的常数M，对任一固定的k，纵然与n无关，但却可以与k有关，很可能选不出对所有 $k\in S$ 都适用的统一的常数 M 来。例如对 $f_k(n)=k/(n^2+k^2)$，对于任意固定的 k，因 $n^2+k^2\geqslant n^2$，故

$$|f_k(n)|\leqslant k/n^2.$$

此即 $f_k(n)=O(n^{-2})$，然而此式对 k 并不是一致的，因为常数 $M=k$ 与 k 有关，因此不能由此推出 $\sum_{k=1}^{n} f_k(n) = \sum O(n^{-2})=O(n^{-1})$. 但若我们改用下列方式估计：

$$(n^2+k^2)=(n-k)^2+2nk\geqslant 2nk,$$

故

$$(k/(n^2+k^2))\leqslant(2n)^{-1},$$

于是 $f_k(n)=O(n^{-1})$，此式关于 k 便是一致的. 因此我们引入定义

定义 2. 设 S 为 k 所取值的某一集合，若存在不依赖于 n 与 $k\in S$ 的常数 a 与 M，使得

$$|a_k(n)|\leqslant M|b_k(n)|$$

对所有满足 $a\leqslant n<+\infty$，$k\in S$ 的n与k均成立，则称 $a_k(n)=O(b_k(n))(n\to\infty)$ 关于 k 是一致的. 又若 $a_k(n)=b_k(n)(1+o(1))$ $(n\to\infty)$，其中隐含在 $o(1)$ 中的常数与 $k\in S$ 的选择无关，则称 $a_k(n)\sim b_k(n)$ 关于 $k\in S$ 是一致的.



由此定义，若 $a_k(n)=O(b_k(n))$ 关于 $k\in S$ 为一致，则必有 $\sum\limits_{k\in S}a_k(n)=O\left(\sum\limits_{k\in S}b_k(n)\right)$. 同样若 $a_k(n)\sim b_k(n)$ 关于 $k\in S$ 为一致，则 $\sum\limits_{k\in S}a_k(n)\sim\sum\limits_{k\in S}b_k(n)$.

在本章以下各节中，我们将介绍渐近计数问题的一些方法。由于计数问题来源的多样性，渐近式的推导方法往往因问题而变，很难纳入几种模式之中，因而我们将只限于介绍最常应用的几种方法。

4.2. 和式变换方法

4.2.1. Stirling 公式及其推论

组合计数问题解的表示式中常包含有阶乘因子 $n!$，为了消去这一因子，我们需要应用 $n!$ 渐近式的著名的 Stirling 公式。本节我们给出这一公式的推导并举例说明如何应用它来求出和式的决定性部分。

首先，由求和公式 (2.5.8) 可以直接推出下列和式的渐近值定理：

定理 A. 设 $f(x)$ 为区间 $[1\ +\infty)$ 上的 $2m$ 阶连续可微函数，且积分 $\int_1^\infty|f^{(2m)}(x)|dx$ 存在，则有渐近值

$$\sum_{k=1}^{n}f(k)=\int_1^n f(x)dx+S+(f(n)/2)$$
$$+\sum_{k=1}^{m}(B_{2k}/(2k)!)f^{(2k-1)}(n)$$
$$+O\left(\int_n^\infty|f^{(2m)}(x)|dx\right),\qquad(1)$$

其中 B_k 为 Bernoulli 数，S 为与 n 无关的常数。



今在(1)式中取 $f(x)=\log x$，注意到 $\int \log x dx = x\log x - x$ 及 $f^{(2k-1)}(x)=(2k-2)!x^{-(2k-1)}$，即得

$$
\begin{aligned}
\log n! = n\log n - n + 1 + S + (\log n)/2 \\
&+ \sum_{k=1}^{m} B_{2k}/(2k(2k-1)n^{2k-1}) \\
&+ O\left(\int_n^{\infty} x^{-2m}dx\right) = (n+1/2)\log n + S_1 \\
&+ \sum_{k=1}^{m-1} B_{2k}/(2k(2k-1)n^{2k-1}) \\
&+ O(n^{-(2m-1)}).
\end{aligned}
$$

取 $m=3$ 即得

$$
\begin{aligned}
n! &= S_2\sqrt{n}(n/e)^n\exp(1/12n \\
&\quad - 1/360n^3 + O(n^{-5})) \\
&= S_2\sqrt{n}(n/e)^n(1+1/12n \\
&\quad + 1/288n^2 + O(n^{-3})). \qquad (2)
\end{aligned}
$$

式中 S, S_1 及 S_2 均为常数，为了定出 S_2，注意到由 Wallis 公式

$$
\begin{aligned}
\frac{\pi}{2} &= \frac{2\cdot 2\cdot 4\cdot 4\cdot 6\cdot 6\cdots\cdots}{1\cdot 3\cdot 3\cdot 5\cdot 5\cdot 7\cdots\cdots} \\
&= \lim_n \frac{2^{4n}(n!)^4}{(2n+1)(2n!)^4},
\end{aligned}
$$

将(2)式代入得

$$
\frac{\pi}{2} = \lim_n \frac{2^{4n}(S_2(n/e)^n\sqrt{n})^4}{(2n+1)(S_2(2n/e)^{2n}\sqrt{2n})^2} = \frac{S_2^2}{4}.
$$

由此 $S_2=\sqrt{2\pi}$，此即证得

定理 B (Stirling 公式).

$$
n! = \sqrt{2\pi n}(n/e)^n(1+1/12n
$$



$$+ 1/288n^2 + O(n^{-3})). \tag{3}$$

顺便指出，和式的渐近值定理A在寻求一类和式的渐近值方面是一个很有用的工具。例如取 $f(x) = 1/x$，即可按类似方式得出

$$\sum_{k=1}^{n} 1/k = \log n + \gamma + (1/2n)$$
$$- (1/12n^2) + O(n^{-4}), \tag{4}$$

其中

$$\gamma = \lim_{n}\left(\sum_{k=1}^{n} 1/k - \log n\right) = 0.57721\cdots$$

称为 **Euler 常数**。渐近式(4)后面也将用到。

求和公式用于渐近计数的例子在下面各节还将提到。下面我们举例指出 Stirling 公式在确定和式 $\sum_{k} a_k(n)$ 的决定性部分中的应用。

作为头一个例子，我们考察二项式系数 $\binom{n}{k}$ $(k = 0, 1, \cdots, n)$。此为一单峰序列，其值开始时随 k 增加，当 $k = [n/2]$ 时达最大值，然后随 k 增大而减小。下面的命题指出当 k 离 $n/2$ 超过一定距离时，$\binom{n}{k}$ 与 $\binom{n}{n/2}$ 相比常可忽略。

命题 1. 记 $j = |n/2 - k|$，则当 $j = o(n)$ 时

$$\binom{n}{k} \sim (2/n\pi)^{1/2} 2^n \exp(-2j^2/n + O(j^3/n^2)). \tag{5}$$

由此尤可推知当 $j \geqslant n^s$, $s > 1/2$ 时

$$\binom{n}{k} = o\left(n^{-p}\binom{n}{n/2}\right), \tag{6}$$

其中 $p > 0$ 为任意固定的正数。



证. 由二项式系数之对称性不妨设 $k<n/2$，即 $j=(n/2)-k$. 应用 Stirling 公式于 $k!$，$(n-k)!$ 及 $n!$，并代入 $\binom{n}{k}=n!/k!(n-k)!$，即易推出

$$\binom{n}{k}=\left(\frac{n}{2\pi k(n-k)}\right)^{1/2}\left(\frac{n}{k}\right)^{k}\times\left(\frac{n}{n-k}\right)^{n-k}\left(1+O\left(\frac{1}{k}+\frac{1}{n-k}\right)\right),$$

代入 $k=n/2-j$ 及 $n-k=n/2+j$，并注意 $j=o(n)$ 即得

$$\left(\frac{n}{k(n-k)}\right)^{1/2}=\left(\frac{n}{(n/2)^2-j^2}\right)^{1/2}$$
$$=\left(\frac{1}{n}\right)^{1/2}\left(1+O\left(\frac{j^2}{n^2}\right)\right),\ \left(\frac{n}{k}\right)^{k}\left(\frac{n}{n-k}\right)^{n-k}$$
$$=\frac{n^n}{((n/2)-j)^{(n/2)-j}((n/2)+j)^{(n/2)+j}}$$
$$=2^n\left(1-\frac{2j}{n}\right)^{j-n/2}\left(1+\frac{2j}{n}\right)^{j+n/2},$$

因此

$$\binom{n}{k}\sim(2/n\pi)^{1/2}2^n(1+2j/n)^{-j-n/2}(1-2j/n)^{j-n/2}.$$

由(4.1.9)

$$(1\pm 2j/n)^{\mp j-n/2}\sim\exp(\mp j-j^2/n+O(j^3/n^2)),$$

因此

$$\binom{n}{k}\sim(2/n\pi)^{1/2}2^n\exp(-2j^2/n+O(j^3/n^2)).$$

(5)式得证. 尤令 $j=0$ 即见

$$\binom{n}{n/2}\sim(2/n\pi)^{1/2}2^n. \tag{7}$$



于是当 $j=o(n)$ 时，

$$\binom{n}{k}\sim\binom{n}{n/2}\exp(-2j^2/n+O(j^3/n^2)). \tag{8}$$

注意到若 $j\geqslant n^s$, $s>\frac{1}{2}$ 但 $j\leqslant n^\delta$, $\delta<2/3$ 时 $j^2/n\to+\infty$, $j^3/n^2\to 0$，并注意 $\exp(-n^\lambda)=o(n^{-p})$，其中 λ, p 为任意正常数，即可见当 $n^\delta\geqslant j\geqslant n^s$, $2/3>\delta\geqslant s>1/2$ 时，

$$\binom{n}{k}=o\left(n^{-p}\binom{n}{n/2}\right).$$

再由 $\binom{n}{k}$ 的单调性可见条件 $n^\delta\geqslant j$ 实际上可以放弃，亦即上式对所有 $j\geqslant n^s$ 均成立。

上面的论证方法是标准的．实际上对于 $a_k(n)$ $(k=0, 1, \cdots, n)$，只要 $a_k(n)$ 是单峰的，即仅在 $k\in\{0, 1, \cdots, n\}$ 之一处达极大值，在其两侧均为单调，而在极大值点邻近有类似于(8)式的渐近值时，都可引出与(6)式相仿的结论．下列两个命题即为例子．

命题 2. 设 $a_k(n)=k^{n-k}k!/n!$，则 $a_k(n)$ 随 k 单调增加，在 $k=n$ 处达到最大值 1；记 $j=n-k$ 为 k 与极值点下标 n 的距离，则当 $j=o(n)$ 时，

$$a_k(n)\sim\exp(-j^2/2n+O(j^3/n^2)). \tag{9}$$

由此尤可推出当 $j\geqslant n^s$, $s>1/2$ 时，对任意正数 p 有

$$a_k(n)=o(n^{-p}).$$

证．因 $a_k(n)/a_{k+1}(n)=(k/k+1)^{n-k}\leqslant 1$，故 $a_k(n)$ 单调增加，在 $k=n$ 处达到最大值 $a_n(n)=1$．记 $j=n-k$，则当 $j=o(n)$ 时，应用 Stirling 公式于 $n!$ 及 $k!$ 并应用(4.1.10)式可知

$$a_k(n)=k^{n-k}k!/n!$$



$$= \sqrt{k/n}\, e^{n-k}(k/n)^n(1 + O(1/n))$$
$$= \sqrt{(n - j)/n}\, e^j(1 - j/n)^n(1 + O(1/n))$$
$$= (1 + O(j/n))e^j \exp(-j - j^2/2n + O(j^3/n^2)),$$

此即(9)式,再由 $a_k(n)$ 之单调性,即见命题为真。

用完全类似的方式可以证明

命题 3. 设 $a_k(n) = n!/((n-k)!n^k)$, 则 $a_k(n)$ 随 k 增加而单调减小, 在 $k = 0$ 处达最大值 1 (此时下标 k 即等于它与极值点下标 $k = 0$ 间的距离),且当 $k = o(n)$ 时,

$$a_k(n) \sim \exp(-k^2/2n + O(k^3/n^2)). \qquad (10)$$

由此尤可推出当 $k \geqslant n^s$, $s > 1/2$ 时,对任意正数 p 有

$$a_k(n) = o(n^{-p}).$$

下面的命题中 $a_k(n)$ 之分析稍见复杂些,但其基本思想与前相同。

命题 4. 设 $a_k(n) = k^n/k!$, 则 $a_k(n)$ 当 $k \approx t$ 时达到极大值,其中 t 满足 $t\log t = n - 1/2$. 又设 $j = |t - k|$ 为 k 与极值点 t 间的距离,则当 $j = o(n^s)$, $s < 2/3$ 时,

$$k^n/k! \sim t^{n-t}e^t(2\pi t)^{-1/2}\exp(-(1 + \log t)j^2/2t). \qquad (11)$$

由此尤可推知,当 $j \geqslant n^s$, $s > 1/2$ 时, $\sum_j a_k(n)$ 可从和式中忽略去, 亦即 $\sum_{j \geqslant n^s} a_k(n) = o\left(\sum_k a_k(n)\right)$.

证. 应用 Stirling 公式可见

$$k^n/k! = (2\pi k)^{-1/2}e^k k^{n-k}(1 + O(1/k)).$$

令 $f(x) = (\sqrt{2\pi x})^{-1}e^x x^{n-x}$, $g(x) = \log f(x)$, 易见 $g'(x)$ 在 $x = t$ 处为零,其中 t 满足 $t\log t = n - 1/2$. 由此易见 $k^n/k!$ 在 $k \approx t$ 处达极大值. 令 $k = t + j$ 即有

$$k^n/k! = (2\pi t)^{-1/2}e^k t^{n-k}(1 + j/t)^{n-k-1/2}(1 + O(1/k)),$$



于是当 $j=o(t)$ 时有

$$k^n/k! \sim (2\pi t)^{-1/2}e^t t^{n-t} e^j t^{-j}(1+j/t)^{t\log t-j-t}.$$

应用与命题 4.1.1 之证明相仿的推理,易证

$$(1+j/t)^{t\log t-j-t} = t^j e^{-j}\exp(-(1+\log t)j^2/2t + O(j^3\log t/t^2)),$$

于是

$$k^n/k! \sim (2\pi t)^{-1/2}e^t t^{n-t}\exp(-(1+\log t)j^2/2t + O(j^3\log t/t^2)).$$

因当 $j=o(n^s)$, $s<2/3$ 时, $j^3\log t/t^2 = o((t^s(\log t)^s)^3 \cdot (\log t)/t^2) = o(t^{3s-2}\log^{s+1}t) = o(1)$, 故此时

$$k^n/k! \sim (2\pi t)^{-1/2}e^t t^{n-t}\exp(-(1+\log t)j^2/2t).$$

4.2.2. 由正项组成的和式

本节考察计数问题的解 $N(n)$ 由正项和式 $\sum_k a_k(n)$ $(a_k(n)>0)$ 表出的情形. 此时 $a_k(n)$ 一般含有阶乘因子,且在区间为单峰(亦即在区间中某一点达极大值,在其两侧为单调), 寻求此种和式渐近值的步骤一般为: (i) 定出求和区间内使 $a_k(n)$ 达最大值的下标 k,为此可将指标 k 视作连续变量,然后应用通常的分析学方法, 也可结合应用 Stirling 公式来近似定出极值位置 t; (ii) 作变量代换 $j=t\pm k$. 新的指标 j 表出了 k 离极值位置 t 的距离. 然后应用 Stirling 公式消去 $a_k(n)$ 中的阶乘因子,并进而分析 $a_k(n)$ 在极值点两侧的增长速度,从中定出对整个和式起决定性影响的部分,亦即推出形如 $\sum_{j>n^s} a_k(n) = o(\sum a_k(n))$ 的估计式;(iii) 估计和式 $\sum_{j\leqslant n^s} a_k(n)$. 常用的工具为 Euler 求和公式,用积分代替和



式．在有些场合也可尝试直接求和．

上面过程中的（i）与（ii）两步在前一小节已列举了数例，故下面将专注于第（iii）步的例释．

例 1. $S_n=\sum_{k=0}^{n}\binom{n}{k}^r\ (r>0)$.

此例中 $a_k(n)=\binom{n}{k}^r$，最大值出现在求和区间的中段 $k=n/2$ 处．作变量代换 $j=n/2-k$（j 从 $-n/2$ 变至 $+n/2$），由命题 1 可知 $\sum_{|j|>n^s}\binom{n}{k}^r$，其中$2/3>s>1/2$可从和式中略去，再由(5)式即见

$$S_n\sim\sum_{|j|<n^s}\binom{n}{k}^r$$

$$\sim(2/n\pi)^{r/2}2^{nr}\sum_{|j|<n^s}\exp(-2r\cdot j^2/n).$$

因当 $|j|\geqslant n^s$，$s>1/2$ 时，$\exp(-2rj^2/n)=o(n^{-p})$，p 为任意正数，故

$$\sum_{|j|<n^s}\exp(-2rj^2/n)$$

$$\sim\sum_{j=-n}^{n}\exp(-2rj^2/n),$$

因此

$$S_n\sim(2/n\pi)^{r/2}2^{nr}\sum_{j=-n}^{n}\exp(-2rj^2/n).$$

令 $f(x)=\exp(-2rx^2/n)$，记 $s_n=\sum_{j=-n}^{n}\exp(-2rj^2/n)=$



$\sum_{j=-n}^{n} f(j)$，应用 Euler 求和公式(2.5.8)得

$$s_n = \int_{-n}^{n} f(x)dx + f(n)/2 + f(-n)/2$$

$$+ \sum_{k=1}^{m} B_{2k}(f^{(2k-1)}(n)$$

$$- f^{(2k-1)}(-n))/(2k)! + R_m, \qquad (12)$$

其中

$$R_m = -\int_{-n}^{n} f^{(2m)}(x) B_{2m}(\{x\})/(2m)!\,dx.$$

(注意此处不能直接引用定理A，因本例 $f(x)$ 与 n 有关，从而(1)式中常数 S 亦将与 n 有关.) 令 $f(x) = g(y) = e^{-y^2}$，$y = \sqrt{2r/n}\,x$，故 $(d/dx)^k f(x) = (\sqrt{2r/n})^k (d/dy)^k e^{-y^2} = (\sqrt{2r/n})^k e^{-y^2} P(y)$，$P(y)$ 为 y 的 k 次多项式. 由此可见(12)式中除积分部分及 R_m 外都等于 $o(n^{-p})$. 而对于余项 R_m 有

$$\int_{-\infty}^{\infty} |f^{(2m)}(x)|\,dx = (\sqrt{2r/n})^{2m-1}$$

$$\times \int_{-\infty}^{\infty} |(d/dy)^{2m} e^{-y^2}|\,dy = O(n^{1/2-m}),$$

因此 $R_m = O(n^{1/2-m})$. 再注意(12)式中的积分 $\int_{-n}^{n} f(x)dx$ 与 $\int_{-\infty}^{\infty} f(x)dx$ 之差为 $O(e^{-bn})$ (b 为某正数)，即见

$$\sum_{j=-n}^{n} f(j) \sim \int_{-\infty}^{\infty} f(x)dx = \sqrt{\pi n/2r}.$$

(右边积分之计算可见 Фихтенгольц [64].) 由此最终得出

$$\sum_{k} \binom{n}{k}^r \sim \left(\frac{2}{n\pi}\right)^{r/2} 2^{nr} \left(\frac{\pi n}{2r}\right)^{1/2}$$



$$= 2^{nr}\left(\frac{2}{n\pi}\right)^{(r-1)/2} r^{-1/2}. \tag{13}$$

例 2. $P(n) = \sum_{k=0}^{n} k^{n-k}\cdot k!/n!$ 及 $Q(n) = \sum_{k=0}^{n} n!/((n-k)!n^k)$.

此两例中，$a_k(n)$ 之最大值出现在求和区间的一端。对于此两和式，由命题 2 和 3，均有

$$P(n),\ Q(n) \sim \sum_{j\leqslant n^\delta} \exp(-j^2/2n).$$

而在前一例中已证得（令 $r=1/4$）上式右边 $\sim \int_0^\infty e^{-x^2/2n}dx = (\sqrt{\pi n/2r})/2 = \sqrt{\pi n/2}$，故

$$P(n),\ Q(n) \sim \sqrt{\pi n/2}.$$

顺便指出，运用更细致的推理可证（见 Knuth [98] V.3）：

$$P(n) = \sqrt{\frac{\pi n}{2}} - \frac{2}{3} + \frac{11}{24}\sqrt{\frac{\pi}{2n}} + \frac{4}{135n} - \frac{71}{1152}\sqrt{\frac{\pi}{2n^3}} + O(n^{-2}),$$

$$Q(n) = \sqrt{\frac{\pi n}{2}} - \frac{1}{3} + \frac{1}{12}\sqrt{\frac{\pi}{2n}} - \frac{4}{135n} + \frac{1}{288}\sqrt{\frac{\pi}{2n^3}} + O(n^{-2}).$$

关于 $P(n)$ 与 $Q(n)$ 的组合学意义，涉及到计算机的算法分析，其中 $P(n)$ 我们将在 6.2 节中再次提到。

例 3. $K(n) = \sum_{k=1}^{n} n!/((n-k)!kn^k)$.

此例中 $K(n)$ 的组合学意义如下：设 F 为 n 个元的集合 S 映于自身的所有映射 f 的集合。对每一 $f\in F$，作出图 G_f，



它以 S 的诸元为顶点，以 $(i, f(i))$，$i\in S$ 为边，则 $K(n)$ 等于当 f 遍及 F 时诸图 G_f 的分支数的平均值.

今往求 $K(n)$ 的渐近值，此例中 $a_k(n) = n!/((n-k)!\, kn^k)$ 与上例 $Q(n)$ 中的 $n!/((n-k)!n^k)$ 仅差因子 $1/k$，故

$$K(n) \sim \sum_{k\leqslant n^\delta} a_k(n) \sim \sum_{k\leqslant n^\delta} (1/k)e^{-k^2/2n}$$

$$\sim \sum_{k=1}^{n} (1/k)e^{-k^2/2n}.$$

但因右边和式中出现因子 $1/k$，这给求和公式的应用带来了困难. 因若令 $f(x) = (1/x)e^{-x^2/2n}$，则 $f(0)$ 没有定义；而若试图用 $\int_1^\infty f(x)dx$ 来逼近，则由于 $1/x$ 之出现，求和公式中的余项易证并不随 n 趋于零. 为了解决这一困难，我们针对 $f(x)$ 在 $x=0$ 处有奇点 $x=0$ 而引入 $g(x) = f(x) - 1/x = (1/x)(e^{-x^2/2n} - 1)$. 此时 $g(0) = 0$，又 $g'(x) = -(1/n)\cdot e^{-x^2/2n} + (1/x^2)(1 - e^{-x^2/2n}) = g_1(x) + g_2(x)$. 显然 $\int_0^n g_1\cdot(x)dx = O(n^{-1})$，而对于 $\int_0^n g_2(x)dx$，作变量代换 $x = \sqrt{2n}y$ 得

$$\int_0^n (1/x^2)(1 - e^{-x^2/2n})dx$$

$$= (1/\sqrt{2n}) \int_0^{\sqrt{n/2}} y^{-2}(1 - e^{-y^2})dy.$$

因 $y^{-2}(1 - e^{-y^2})$ 在 $y=0$ 处取值为 1，故可见上式为 $O(n^{-1/2})$. 于是应用求和公式

$$\sum_{k=0}^{n} g(k) = \int_0^n g(x)dx + (g(0) + g(n))/2$$



$$+\int_0^n B_1(\{x\})g'(x)dx.$$

注意到 $g(n)=O(n^{-1})$, $g(0)=0$, 又

$$\left|\int_0^n B_1(\{x\})g'(x)dx\right| \leqslant \int_0^n |g'(x)|dx = O(n^{-1/2}),$$

故

$$\sum_{k=0}^{n} g(k) = \int_0^n g(x)dx + O(n^{-1/2}).$$

此即

$$\sum_{k=0}^{n} (1/k)(e^{-k^2/n}-1)$$

$$=\int_0^n (1/x)(e^{-x^2/2n}-1)dx + O(n^{-1/2}).$$

对于右端的积分,令 $y=x^2/2n$, 则

$$\int_0^n (1/x)(e^{-x^2/2n}-1)dx$$

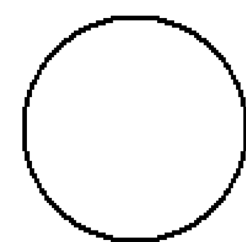
$$=(1/2)\int_0^{n/2}(1/y)(e^{-y}-1)\,dy$$

$$=(1/2)\int_0^1 (1/y)(e^{-y}-1)dy$$

$$+(1/2)\int_1^\infty y^{-1}e^{-y}dy$$

$$-(1/2)\int_{n/2}^\infty y^{-1}e^{-y}dy$$

$$-(1/2)\int_1^{n/2} y^{-1}dy.$$



但

$$\int_0^1 y^{-1}(e^{-y}-1)dy + \int_1^\infty e^{-y}y^{-1}dy = \gamma, \qquad (14)$$

其中 γ 为 Euler 常数。((14)式之证可见 Фихтенгольц [64].)
而



$$\int_{n/2}^{\infty} y^{-1}e^{-y}dy \leqslant (2/n)\int_{n/2}^{\infty} e^{-y}dy$$
$$= (2/n)e^{-n/2} = o(e^{-n/2}),$$

又 $\int_1^{n/2} y^{-1}dy = \log(n/2)$，故

$$\int_0^{n/2} (1/x)(e^{-x^2/2n} - 1)dx$$
$$= -\gamma/2 - (1/2)\log(n/2) + o(e^{-n/2}).$$

由此注意到 $\sum_{k=1}^{n}(1/k) = \log n + \gamma + O(n^{-1})$（见(4)式），故

$$\begin{aligned}\sum_{k=1}^{n}(1/k)e^{-k^2/2n} &= \sum_{k=1}^{n}(1/k)(e^{-k^2/2n} - 1) + \sum_{k=1}^{n}(1/k) \\ &= -(\gamma/2) - (1/2)\log(n/2) \\ &\quad + \log n + \gamma + O(n^{-1/2}) \\ &= (\log n)/2 + (\gamma + \log 2)/2 \\ &\quad + O(n^{-1/2}).\end{aligned}$$

于是最终得出

$$K(n) \sim (\log n)/2 + (\gamma + \log 2)/2.$$

我们还可以用另一种方法——分部求和法来求出 $\sum(1/k)e^{-k^2/2n}$ 之渐近值.一般,若我们需要寻求 $\sum_{i=1}^{n} a_ib_i$ 之渐近值,其中 $\sum_{i=1}^{n} a_i$ 之渐近值已经知道,而与 $b_i = b(i)$ 相应的函数 $b(x)$ 又比较光滑，则可尝试用 **Abel 分部求和公式**

$$a_1b_1 + \cdots + a_nb_n = A_nb_n - \sum_{k=1}^{n-1} A_k(b_{k+1} - b_k), \tag{15}$$



其中 $A_k = \sum_{i=1}^{k} a_i$.其证如下:定义 $A_0 = 0$, 于是 $a_k = A_k - A_{k-1}$,

$$\begin{aligned}\sum_{k=1}^{n} a_k b_k &= \sum_{k=1}^{n} A_k b_k - \sum_{k=1}^{n} A_{k-1} b_k \\ &= \sum_{k=1}^{n} A_k b_k - \sum_{k=0}^{n-1} A_k b_{k+1} \\ &= A_n b_n - A_0 b_1 - \sum_{k=1}^{n-1} (A_k b_{k+1} - A_k b_k) \\ &= A_n b_n - \sum_{k=1}^{n-1} A_k (b_{k+1} - b_k).\end{aligned}$$

若应用差分算子 Δ 与 ∇,(15)式也可写成

$$\begin{aligned}\sum_{k=1}^{n} b_k(\nabla c_k) = b_n c_n - b_1 c_0 \\ - \sum_{k=1}^{n} c_k(\Delta b_k).\end{aligned}$$

这与分析学中的分部积分公式完全相仿.(15)式在分析学中有重要的应用(见徐利治[8]).

(15)式还可改写成积分形式,为此记 $A(x) = \sum_{k\leqslant x} a_k$,于是当 $k \leqslant x < k+1$ 时,$A(x) = A_k$,故

$$\begin{aligned}\sum_{k=1}^{n-1} A_k(b_{k+1} - b_k) &= \sum_{k=1}^{n-1} A_k \int_k^{k+1} b'(x)dx \\ &= \sum_{k=1}^{n-1} \int_k^{k+1} A(x)b'(x)dx = \int_1^n A(x)b'(x)dx.\end{aligned}$$

于是有

$$a_1 b_1 + \cdots + a_n b_n = A_n b_n - \int_1^n A(x)b'(x)dx. \quad (16)$$



今应用 (16) 式求本例 $K(n)$ 之渐近式. 如前所述, $K(n) \sim E(n)$, 其中 $E(n)$ 定义为

$$E(n) = \sum_{k=1}^{n}(1/k)e^{-k^2 t} \quad (t = 1/2n).$$

今在(16)式中取 $a_k = 1/k$, $b_k = e^{-k^2 t}$, 于是

$$A(x) = \sum_{k \leqslant x} a_k = \log x + \gamma + O(x^{-1}),$$

$$E(n) = A(n)A_n - \int_1^n A(x)b'(x)dx$$

$$= A(n)b_n - \int_1^n (\log x + \gamma + O(x^{-1}))b'(x)dx.$$

因

$$-\gamma \int_1^n b'(x)dx = -\gamma b(x) \Big|_1^n$$

$$= \gamma b(1) + O(e^{-n/2})$$

$$= \gamma e^{-t} + O(e^{-n/2}) = \gamma + O(n^{-1}),$$

$$A(n)b_n = A(n)e^{-n/2} = O(e^{-bn}) \quad (b > 0),$$

$$O\left(\int_1^n x^{-1}b'(x)dx\right) = O\left(t\int_1^\infty e^{-x^2 t}dx\right)$$

$$= O\left(\sqrt{t}\int_{\sqrt{t}}^\infty e^{-y^2}dy\right) = O(\sqrt{t})$$

$$= O(n^{-1/2}),$$

所以

$$E(n) = \gamma - \int_1^\infty (\log x)b'(x)dx + O(n^{-1/2}).$$

今

$$-\int_1^\infty (\log x)b'(x)dx = \log x b(x) \Big|_1^\infty + \int_1^\infty (b(x)/x)dx = \int_1^\infty x^{-1}e^{-x^2 t}dx.$$



作代换 $x^2t=u$，于是 $dx/x=du/2u$。

$$\int_1^\infty x^{-1}e^{-x^2t}dx=(1/2)\int_t^\infty u^{-1}e^{-u}du$$

$$=(1/2)\left(\int_t^1(e^{-u}-1)/u\,du\right.$$

$$\left.+\int_1^\infty u^{-1}e^{-u}du+\int_t^1 u^{-1}du\right)$$

$$=(1/2)\left(\int_0^1(e^{-u}-1)/u\,du\right.$$

$$\left.+\int_1^\infty u^{-1}e^{-u}du-\log t+O(t)\right).$$

由(14)式可见上式等于 $(1/2)(-\gamma-\log t+O(t))$，因此

$$E(n)=\gamma+(1/2)(-\gamma-\log t)+O(t^{1/2}).$$

代入 $t=1/2n$ 即得

$$K(n)=(1/2)(\gamma+\log 2n)+O(n^{-1/2}),$$

与前面所得一致.

例 4. Bell 数(2.3.14) $Y_n=e^{-1}\sum_{k=1}^{n}k^n/k!$.

由命题 4

$$\sum_{k=0}^{\infty}k^n/k!\sim\sum_{|j|<n^s}f(j),$$

其中 $1/2<s<2/3$，$f(j)=t^{n-t}e^t(2\pi t)^{-1/2}\exp(-(1+\log t)j^2/2t)$，其中 t 由 $t\log t=n-1/2$ 决定. 应用求和公式于 $f(j)=ce^{-aj^2}$ 可见

$$(e^{-1})\sum_k k^n/k!\sim\int_{-\infty}^{\infty}t^{n-t}e^t(2\pi t)^{-1/2}$$

$$\times\exp(-(1+\log t)x^2/2t)dx.$$

注意到 $\int_{-\infty}^{\infty}e^{-a^2x^2}dx=\sqrt{\pi}/a$（见 Фихтенгольц [64]），故

$$Y_n\sim t^{n-t}e^{t-1}(2\pi t)^{-1/2}\sqrt{\pi}/\sqrt{(1+\log t)/2t}$$



$$\sim t^{n-t}e^{t-1}(\log t)^{-1/2}. \tag{17}$$

此式尚可进一步变换成右边显含 n 的形式。为此先在两边取对数得

$$\log Y_n \sim (n-t)\log t + (t-1) - (\log t)/2.$$

右边等于 $(n-1/2)\log t - t\log t + (t-1) = (n-1/2)\cdot(\log t - 1) + (t-1)$，因此

$$\begin{aligned}(\log Y_n)/n &\sim \log t - 1 + (t-1)/(n-1/2)\\ &= \log t - 1 + (1/\log t) + O(1/t\log t).\end{aligned} \tag{18}$$

今用迭代方法从方程 $t\log t = n - 1/2$ 中解出 $t = t(n)$。为此记 $x = n - 1/2$，在 $t\log t = x$ 两边取对数，并置 $\log t = y$，即有 $y + \log y = \log x$，或

$$y = \log x - \log y. \tag{19}$$

当 $x = n - 1/2 \to +\infty$ 时，显然 $y \to \infty$，故可见 $y > 1$，但此时 $y = \log x - \log y < \log x$，故 $1 < y < \log x$，由此 $\log y = O(\log\log x)$ 代入(19)式可见

$$\begin{aligned}y &= \log x + O(\log\log x)\\ &= \log x(1 + O(\log\log x/\log x)),\end{aligned}$$

两边取对数得

$$\begin{aligned}\log y &= \log\log x + \log(1 + O(\log\log x/\log x))\\ &= \log\log x + O(\log\log x/\log x).\end{aligned}$$

再次代入(19)式可见

$$\begin{aligned}y &= \log x - \log\log x + O(\log\log x/\log x)\\ &= \log x(1 - \log\log x/\log x\\ &\quad + O(\log\log x/(\log x)^2)),\end{aligned}$$

复将此式取对数，重复上述过程即得

$$\begin{aligned}y = \log x &- \log\log x + \log\log x/\log x\\ &+ (1/2)(\log\log x/\log x)^2\\ &+ O(\log\log x/(\log x)^2).\end{aligned}$$



由此

$$1/y = (1/\log x)(1 + O(\log\log x/\log x))^{-1}$$
$$= (1/\log x) + O(\log\log x/(\log x)^2).$$

将上两式代入(18)式即最终得到

$$(\log Y_n)/n \sim \log n - \log\log n - 1 + \log\log n/\log n$$
$$+ (1/\log n) + (1/2)(\log\log n/\log n)^2$$
$$+ O(\log\log n/(\log n)^2). \tag{20}$$

Y_n 渐近式的另一种求法乃利用生成函数 $\exp(e^x-1)=\Sigma Y_n x^n/n!$，详见第三节.

4.2.3. 由交错项组成的和式

对于由交错项组成的和式 $N=\sum_k(-1)^k a_n(k)$，$a_n(k)\geqslant 0$，一般由于正负项之间的抵销作用，N常比各项绝对值之和 $\sum_k a_n(k)$ 要小得多，因而其处理往往比正项和式的情形更为困难．若分别估计 $N_1=\sum_k a_n(2k)$ 及 $N_2=\sum_k a_n(2k+1)$，则由于 N_1 与 N_2 常渐近相等，很难估计其差 $N=N_1-N_2$ 的渐近式．因此，一般的作法是设法将N转换为正项和式的情形．例如当 $a_n(k)$ 为单调减的情形，可将和式写成 $\Sigma(a_n(2k)-a_n(2k+1))$，此时若 $a_n(x)$ 为光滑函数时，还可用 $-a_n'(2k)=-(d/dx\,a_n(x))_{x=2k}$ 作为 $a_n(2k)-a_n(2k+1)$ 的近似．在有些场合，针对和式的特点可以作出其它形式的变换．关于这些带普适性的方法，本节不再细述，读者可参阅 de Bruijn [41] 中的例子．对于由组合计数问题引出的交错项和式，一般若能找到问题的生成函数，则从生成函数出发往往更为简便，但很多由交错项和式表出的组合计数问题的解，通常系应用入与出原理得来，很难找到相应的生



成函数，因而需要一种直接从此种和式引出渐近式的方法．在这方面，下列不等式(见 Feller [63])是一个很有用的工具．

定理 C (Bonferroni 不等式)．设 A 为 n 个元的集合，$P=\{p_1,\cdots,p_m\}$ 为 m 个性质之集合，记

$$P_=(k)=\sum_{X\subset P,|X|=k}N_=(X),\quad S_k=\sum_{X\subset P,|X|=k}N_\geqslant(X)$$

($N_=(X)$，$N_\geqslant(X)$ 之定义见 3.4 节)，则

$$\left|P_=(k)-\sum_{j<t}(-1)^j\binom{k+j}{j}S_{k+j}\right|\leqslant\binom{k+t}{t}S_{k+t}. \tag{21}$$

注意到当 $k+t>m$ 时，$S_{k+t}=0$，上式便化作通常的筛法公式(3.4.10)．

证．由(3.4.10)式

$$P_=(k)=\sum_{j=k}^m(-1)^{j-k}\binom{j}{k}S_j, \tag{22}$$

因此

$$\left|P_=(k)-\sum_{j=k}^u(-1)^{j-k}\binom{j}{k}S_j\right|$$

$$=\left|\binom{u+1}{k}S_{u+1}-\sum_{j=u+2}^m(-1)^{j-u}\binom{j}{k}S_j\right|.$$

于是为证(21)式，只须证明对任意的 s 均有

$$\sum_{j=s}^m(-1)^{j-s}\binom{j}{k}S_j\geqslant 0.$$

为此注意(22)式，应用与(3.1.4)之证相仿的推理得

$$S_j=\sum_{i=j}^m\binom{i}{j}P_=(i),$$

因此



$$\begin{aligned}\sum_{j=s}^{m}(-1)^{j-s}\binom{j}{k}S_j &= \sum_{j=s}^{m}(-1)^{j-s}\binom{j}{k}\sum_{i=j}^{m}\binom{i}{j}P_=(i)\\ &= \sum_{i=s}^{m}\left(\sum_{j=s}^{i}(-1)^{j-s}\binom{j}{k}\binom{i}{j}\right)P_=(i)\\ &= \sum_{i=s}^{m}\binom{i-k-1}{s-k-1}P_=(i)\geqslant 0.\end{aligned}$$

证毕.

利用上述不等式，可经下列步骤来估计用入与出原理导出来的和式：(i) 估计(21)式左边和式中的一般项；(ii) 估计(21)右边所给出的误差项,由此得出对 $P_=(k)$ 的估计;(iii) 证明在 (i) 与 (ii) 两步中引出的误差项与 $P_=(k)$ 本身的估计式相比可以忽略（通常可以限定某些参数的取值范围来达到这一目的）.

下面的推论给出了在很多情形中能方便地定出渐近值的方法(见 Bender [33]).

推论. 若存在函数 $f(n)$ 及有界函数 $\lambda(n)\geqslant 0$, 使得

$$r!S_r \sim f(n)\lambda(n)^r \tag{23}$$

对 $0\leqslant r\leqslant l(n)$ 一致成立,其中 $l(n)$ 为随 n 趋于无穷的某个函数,则

$$P_=(k)\sim f(n)e^{-\lambda(n)}\lambda(n)^k/k! \tag{24}$$

对 $0\leqslant k\leqslant m(n)$ 一致成立，这里 $m(n)$ 的选取应满足条件：$l(n)-m(n)$ 随 n 趋于无穷.

证. 在(21)中取 $t=l(n)-k$, 则由(23)式可见

$$\sum_{j<t}(-1)^j\binom{k+j}{j}S_{k+j}\sim\sum_{j<t}(-1)^j$$



$$\times \binom{k+j}{j} f(n)\lambda(n)^{k+j}/(k+j)!$$

$$= (f(n)\lambda(n)^k/k!) \sum_{j<t} (-\lambda(n))^j/j!.$$

因 $\lambda(n)$ 有界,故由 e^x 的带余项的 Taylor 展开式可见

$$\sum_{j<t} (-1)^j \binom{k+j}{j} S_{k+j} \sim f(n)e^{-\lambda(n)}\lambda(n)^k/k!.$$

而(21)式的右边渐近等于 $f(n)\lambda(n)^{k+t}/k!t! = (f(n)\lambda(n)^k/k!)(\lambda(n)^t/t!)$, 注意到 $t = l(n) - k \geqslant l(n) - m(n) \to \infty$,故 $\lambda(n)^t/t! = o(1)$. 故

$$P_=(k) = f(n)e^{-\lambda(n)}(\lambda(n)^k/k!)(1 + o(1)).$$

证毕.

例 **1** (分放问题). 将 m 个编了号的球分放到 n 个编了号的盒子中去,使得恰有 k 个盒子是空的,求此种分放方式个数 $a_k(m, n)$ 的渐近值 $(n \to \infty)$.

记性质 p_j 为"第 j 个盒子是空的" $(1 \leqslant j \leqslant n)$, 则满足性质 $p_{j_1}, p_{j_2}, \cdots, p_{j_k}$ 的分放方式显然为 $(n-k)^m$, 因为此时 m 个球可以放入除盒子 $j_1, \cdots, j_k$ 外的任一盒子之中, 因此每个球都有 $(n-k)$ 种放法. 于是 $S_r = \binom{n}{r}(n-r)^m$.

从而

$$a_k(m, n) = \sum_{j=k}^{m} (-1)^{j-k} \binom{j}{k} \binom{n}{j} (n-j)^m.$$

应用 Stirling 公式及 (4.1.9) 式易证当 $r^2 = o(n)$ 及 $mr^2 = o(n^2)$ 时,

$$rS_r \sim n^m(ne^{-m/n})^r,$$

因此由推论(23)可见,若 $ne^{-m/n}$ 有界,则有渐近式

$$a_k(m,n) \sim (n^m/k!)(ne^{-m/n})^k \exp(-ne^{-m/n}).$$



例 2 (对子问题). (见 3.4 节)以 $T(n)$ 记满足 $\pi(i) \not\equiv i, i+1 \pmod n$ 的 n-排列 $\pi=(\pi(1), \cdots, \pi(n))$ 的个数,则

$$T(n)=\sum_{k=0}^{n}(-1)^k(2n/(2n-k))\binom{2n-k}{k}(n-k)!.$$

此例中

$$S_k=(2n/(2n-k))\binom{2n-k}{k}(n-k)!,$$
$$T(n)=P_{=}(0).$$

应用 Stirling 公式及(4.1.9)式易证当 $k<n^\delta$, $\delta<1/2$ 时,

$$\begin{aligned} k!S_k &\sim (\sqrt{2\pi n}\, e^{-n}n^n)2^k \\ &\quad \times (1-k/2n)^{2n-k}(1-k/n)^{-n+k} \\ &\sim (\sqrt{2\pi n}\, e^{-n}n^n)2^k. \end{aligned}$$

此即 $f(n)=\sqrt{2\pi n}\,(n/e)^n$, $\lambda(n)=2$, 故

$$T(n)=P_{=}(0)\sim\sqrt{2\pi n}\,(n/e)^n e^{-2}\sim n!\,e^{-2}.$$

4.3. 生成函数方法

生成函数方法不仅有助于寻求计数问题解的显式,而且在渐近计数方面也是一个十分有用的工具,从生成函数出发通常比直接从和式出发更易得出解的渐近式.本节将分三小节分别讨论生成函数有奇性、无奇性及用函数方程隐式给出的情形.生成函数方法涉及到复变函数论中的有关结果,限于篇幅,我们将直接引述这些结果本身而不作任何证明.

4.3.1. 生成函数有奇性的情形

我们区分两种不同类型的奇点: 代数奇点与非代数奇



点．若生成函数 $f(z)=\Sigma a_n z^n$ 有奇点 α，在其邻近 $f(z)$ 可写成 $g(z)/(1-z/\alpha)^\omega$ 的形式，其中 $g(z)$ 在 α 的邻近解析且异于零，ω 为正实数，则称 α 为 $f(z)$ 的 ω 级代数奇点，在 $f(z)$ 仅有代数奇点时，运用下面的 Darboux 定理（见 Szegö [150]）在很多场合可以引出 a_n 的渐近性态．

定理 A. 设 $f(z)=\sum_{n\geq 0} a_n z^n$ 在 $|z|<r$ 内解析，在 $|z|=r$ 上仅有有限个代数奇点，设它们中间具最高级 ω 的奇点分别为 $\alpha_1, \alpha_2, \cdots, \alpha_m$，则

$$a_n=(n^{\omega-1}/\Gamma(\omega))\times\left(\sum_{k=1}^{m} g_k(\alpha_k)\alpha_k^{-n}+o(r^{-n})\right), \qquad (1)$$

其中 $\Gamma(\omega)$ 为伽马函数，$g_k(z)$ 为与奇点 α_k 相应的函数 $g(z)$，亦即

$$g_k(\alpha_k)=\lim_{z\to\alpha_k}(1-(z/\alpha_k))^\omega f(z). \qquad (2)$$

例 1. Bernoulli 数 B_n（见 3.5 节），其指数生成函数为 $B(z)=\sum B_n z^n/n!=z/(e^z-1)$，分母 e^z-1 的零点为 $2\pi k i\times(i=\sqrt{-1})$，$k=0, \pm1, \pm2, \cdots$．但易见 $z=0$ 非 $B(z)$ 的奇点，故 $B(z)$ 在 $|z|<2\pi$ 中解析，在 $|z|=2\pi$ 上有两个一次极点 $z=\pm 2\pi i$，$\omega=1$，应用定理 A，此时

$$g(\alpha_1)=\lim_{z\to 2\pi i}(z/(e^z-1))(1-z/2\pi i)$$
$$=(-1/2\pi i)\left(z\Big/\frac{d}{dz}e^z\right)_{z=2\pi i}=-1.$$

同样 $g(\alpha_2)=-1$，注意到 $\Gamma(1)=1$，便得

$$B_n/n!=(-1/(2\pi i)^n)+(-1/(-2\pi i)^n)+o((2\pi)^{-n})$$
$$=(-1/(2\pi i)^n)(1+(-1)^n)+o((2\pi)^{-n}).$$



当 $n=2m$ 时便得

$$B_{2m}\sim(-1)^{m-1}(2m)!/(2\pi)^{2m}. \tag{3}$$

而当 $n=2m+1$ 时，由于正负项相消，我们只能得出 $B_{2m+1}=o((2m+1)!/(2\pi)^{2m+1})$. 事实上此时 $B_{2m+1}=0$. 由此例可见(1)式仅当和式中各主要项互不相消时才给出 a_n 之渐近式.

例 2. 由 n 个编了号的顶点 $x_1,\cdots,x_n$ 构成的图 G，若过每一点 x_i 均有 r 条边，则称为 **r 次正则图**. 以 $G(n,r)$ 记此种图的个数. 显然 0 次正则图由 n 个孤立点组成，从而 $G(n,0)=1$. 而每个 1 次正则图相应于 n 个点的两两配对的一种方式. 例如 $n=4$ 时，4 个点共有 3 种配对方式 $\{1,2\},\{3,4\};\{1,3\},\{2,4\};\{1,4\},\{2,3\}$，故 $G(4,1)=3$. 一般易证 $G(2m+1,1)=0$，$G(2m,1)=\binom{2m}{2,2,\cdots,2}\Big/m!=(2m)!/(2^m m!)$. 对于 $G(n,2)=a_n$，则需作较细的讨论，在 Comtet [51] 中从求出其递推式入手导出了它的指数生成函数为

$$\begin{aligned}f(z)&=\sum_{n=0}^{\infty}a_nz^n/n!\\&=(1-z)^{-1/2}\exp(-(z^2+2z)/4).\end{aligned}$$

此级数在 $|z|<1$ 中收敛，在 $|z|=1$ 上有一代数奇点 $\alpha=1$, $\omega=1/2$，相应的

$$\begin{aligned}g(\alpha)&=\lim_{z\to1}\sqrt{1-z}\,f(z)\\&=\exp(-(z^2+2z)/4)_{z=1}=e^{-3/4}.\end{aligned}$$

故由定理 A，注意到 $\Gamma(1/2)=\sqrt{\pi}$，可得

$$G(n,2)\sim n!\,e^{-3/4}(n\pi)^{-1/2}.$$



再应用 Stirling 公式可见

$$G(n,2)\sim\sqrt{2}\,e^{-3/4}(n/e)^n. \tag{4}$$

例 3. Fibonacci 数(见 2.1 节), F_n: $F_0=F_1=1, F_{n+2}=F_{n+1}+F_n$. 其生成函数 $F(z)=\sum_n F_n z^n$ 等于

$$F(z)=(1-z-z^2)^{-1}.$$

分母有根 $\alpha_1=(\sqrt{5}-1)/2$ 及 $\alpha_2=-(\sqrt{5}+1)/2$, $|\alpha_1|<|\alpha_2|$. 由此可见 $F(z)$ 在 $|z|=\alpha_1$ 上有一次极点 $z=\alpha_1$, 而 $g(\alpha_1)=\lim_{z\to\alpha_1}(1-z/\alpha_1)F(z)=(1-\alpha_1/\alpha_2)^{-1}=-\alpha_2/\sqrt{5}$,注意到 $\alpha_1^{-1}=-\alpha_2$, 故由定理 A

$$\begin{aligned}F_n&\sim(-\alpha_2)^{n+1}/\sqrt{5}\\&=((\sqrt{5}+1)/2)^{n+1}/\sqrt{5}.\end{aligned} \tag{5}$$

将上述推导方式加以推广,便可导出当计数问题解 a_n 满足 $a_{n+m}=\sum_{k=0}^{m-1}c_k a_{n+k}$, 其中 c_k, m 为常数时 a_n 的渐近式. 但当 $c_k=c_k(n)$ 与 n 有关,或 m 随 n 一起趋于无穷时,情形比较复杂,是一个有待深入的课题.

例 4. 第二类 Stirling 数 $S(n,k)$ (见 2.4 节), 它的寻常生成函数为

$$\begin{aligned}G_k(z)&=\sum_n S(n,k)z^n\\&=z^k/((1-z)(1-2z)\cdots(1-kz)),\end{aligned}$$

由此易见绝对值最小的奇点为 $\alpha=1/k$, $\omega=1$,相应的 $g(\alpha)$ 等于

$$\lim_{z\to 1/k}(1-kz)G_k(z)=1/k!.$$

故由定理 A

$$S(n,k)\sim k^n/k!. \tag{6}$$



此式也可直接从 $S(n,k)$ 的表示式(2.3.11)得出。在 Jordan [91] 中,从 $S(n+k,n)$ 的另一种和式出发证得

$$S(n+k,n)\sim n^{2k}/(k!2^k). \qquad (7)$$

但上述两个渐近式(6)与(7)中 k 均为固定,当 k 随 n 趋于无穷时,详细的讨论可见 Moser and Wyman [113]。这里顺便提及第一类 Stirling 数 $s(n,k)$ 的渐近式。Jordan 首先证明当 k 固定时

$$|s(n,k)|\sim(n-1)!(\log n+\gamma)^{k-1}/(k-1)!, \qquad (8)$$

其中 γ 为 Euler 常数。至于 $1\leqslant k\leqslant n$ 中的各种 k 值情形,详细讨论可见 Moser and Wyman [114]。

例 5. 不定方程 $\sum_{i=1}^{m}a_ix_i=n$,其中 $\gcd(a_1,\cdots,a_m)=1$,的非负解个数 N_n。已知 N_n 的生成函数为(见例(2.2.4))

$$N(z)=\sum_n N_nz^n=((1-z^{a_1})(1-z^{a_2})\cdots(1-z^{a_m}))^{-1},$$

其奇点 $\alpha=1$, $\omega=m$,易计得 $g(\alpha)=(a_1a_2\cdots a_m)^{-1}$,故

$$\begin{aligned}N_n&\sim(n^{m-1}/\Gamma(m))(a_1\cdots a_m)^{-1}\\&=n^{m-1}/((m-1)!a_1\cdots a_m).\end{aligned} \qquad (9)$$

对于非代数奇点情形,由于情形比较复杂,迄今结果不多,我们只给出下面的定理

定理 B. 设 a_n 的寻常生成函数 $f(z)=\sum a_nz^n$ 为

$$f(z)=\prod_{m\geqslant1}(1-z^m)^{-b_m},$$

其中 $b_1\geqslant1$, $b_m\geqslant0$,又

$$\sum_{m\leqslant x}b_m\sim Kx^u(\log x)^v \quad (u>0), \qquad (10)$$

则

$$\log a_n\sim c(n^u(\log n)^v)^{1/(u+1)},$$

其中常数



$$C = u^{-1}(Ku(u+1)^{u-v}\Gamma(u+2)\zeta(u+1))^{1/(u+1)},$$
$\Gamma(u)$ 为伽马函数，$\zeta(u)$ 为采他函数。

此外，条件 $b_1 \geqslant 1$ 也可以用下面两个条件取代之：(i) 若 $b_m \neq 0$，则 $b_m \geqslant 1$；(ii) 所有充分大的整数 n 都可以表示成使 $b_m \neq 0$ 的诸 m 之和(m 可以重复)。

例 6 (**数的分划问题**). 设 n 为正整数，每一种形如

$$n = y_1 + y_2 + \cdots + y_m,$$

其中 $y_1 \geqslant y_2 \geqslant \cdots \geqslant y_m \geqslant 1$，$m \geqslant 1$，称为 n 的一个分划. n 的全部分划个数记作 $p(n)$. 例如 $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$，故 $p(4) = 5$，易见 $p(n)$ 等于不定方程

$$x_1 + 2x_2 + \cdots + nx_n = n, \qquad x_i \geqslant 0$$

的解的个数，实际上此处 x_i 等于前一方程的解 $y_1, \cdots, y_m$ 中等于 i 的个数。由此易见 $p(n)$ 的生成函数等于

$$f(z) = \prod_{k \geqslant 1} (1 - z^k)^{-1}.$$

此时(10)式中的 $K = 1$，$v = 0$，故注意到 $\zeta(2) = \sum 1/n^2 = \pi^2/6$ (见命题(2.5.3))，即得

$$\log p(n) \sim \pi\sqrt{2n/3}. \tag{11}$$

注意，应用定理 B 只得出 $\log p(n)$ 的渐近值. 在解析数论中已证得

$$p(n) \sim (1/(4n\sqrt{3}))\exp(\pi\sqrt{2n/3}).$$

较之 $p(n)$ 更一般的分划问题乃不定方程

$$n = a_1x_1 + a_2x_2 + \cdots \quad (a_i \in S,\ x_i \geqslant 0)$$

的解的个数 N_n，其中 S 为某个正整数的有限或无限集. 当 S 为有限时见于例 5. 易见 N_n 的生成函数 $\sum N_n z^n$ 等于

$$\prod_{k \in S} (1 - z^k)^{-1}.$$



当 S 取作所有素数的集合时，由著名的素数定理 $\pi(x) \sim x/\log x$，故在定理 B 中取 $K=1$，$u=1$，$v=-1$，于是

$$\log N_n \sim 2\pi\sqrt{n/(3\log n)}. \tag{12}$$

4.3.2. 生成函数无奇点情形

当生成函数不具有奇点（指有限奇点）亦即为整函数时，最简单的形式是 $f(z)=e^{P(z)}$，其中 $P(z)$ 为多项式

$$P(z)=\sum_{k\in S} a_k z^k \quad (a_k>0), \tag{13}$$

S 为某个有限的正整数集合：$S=\{r,s,\cdots,m\}$. 我们可以假设 S 中诸元的最大公约数等于 1，

$$\gcd\{r,s,\cdots,m\}=1, \tag{14}$$

在 $\gcd\{r,s,\cdots,m\}=q>1$ 的情形，只需作代换 $w=z^q$ 便化至上述情形，对于此种形式的整函数可见 Moser and Wyman [112].

定理 C. 设 a_n 的指数生成函数 $f(z)=\sum a_n z^n/n!=e^{P(z)}$，其中 $P(z)$ 为多项式(13)，并满足条件(14)，则

$$a_n \sim n!\,e^{P(r)}/(r^n\sqrt{2\pi c(r)}), \tag{15}$$

其中 r 由方程

$$rP'(r)=n \tag{16}$$

确定，而

$$c(r)=\sum k^2 a_k r^k=(rd/dr)^2 P(r). \tag{17}$$

例 7. 考察 n 个文字之对称群（定义详见 5.1 节）. 以 $a_n(p)$ 表示 S_n 中满足 $\sigma^p=e$ 的置换个数，其中 e 为单位置换，p 为素数. 易证 $a_n(p)$ 的指数生成函数为 $e^{P(z)}$，$P(z)=z+z^p/p$. 由定理 C 即见

$$a_n(p) \sim n!\exp(r+r^p/p)/(r^n\sqrt{2\pi(r+pr^p)}\,), \tag{18}$$



其中 r 满足 $rp'(r) = r + r^p = n$，于是 $\exp(r^p/p) =$ $\mathrm{txp}((n/p) - (r/p))$，

$$r^n = (n - r)^{n/p} = n^{n/p}(1 - r/n)^{n/p}$$
$$\sim n^{n/p}\exp(-(r/p) - (r^2/2pn)),$$

又

$$(r + pr^p)^{1/2} \sim (pn)^{1/2},$$

代入(18)式并约去因子 $\exp(-r/p)$，应用 Stirling 公式即得

$$a_n(p) \sim \frac{n!\exp(r + n/p - r/p)}{n^{n/p}\exp(-r/p - r^2/2pn)\sqrt{2\pi np}}$$
$$\sim (n/e)^{n(1-1/p)}p^{-1/2}\exp(r + r^2/2pn).$$

今分两种情形考察：当 $p = 2$ 时，$r^2 + r = n$，故 $r = (\sqrt{4n+1} - 1)/2 \sim \sqrt{n} - 1/2$，故

$$r^2/2pn = (n - r)/2pn$$
$$= 1/2p - r/2pn \sim 1/2p = 1/4.$$

于是

$$\exp(r + r^2/2pn) \sim e^{\sqrt{n} - 1/4},$$

因此

$$a_n(2) \sim (n/e)^{n/2}2^{-1/2}\exp(\sqrt{n} - 1/4). \tag{19}$$

当 $p > 2$ 时，$r + r^2/2np \sim r \sim n^{1/p}$，故

$$a_n(p) \sim (n/e)^{n(1-1/p)}p^{-1/2}\exp(n^{1/p}). \tag{20}$$

定理C中所述的函数类，因要求 $p(z)$ 为多项式，对于组合计数问题应用而言还嫌太窄。例如对 Bell 数 Y_n（它的生成函数为 $\exp(e^z - 1)$）就不能适用。Hayman 在[84]中将定理适用的范围作了扩大，他引入了一类称为"允许函数"的整函数（下面记此类函数为 $\mathscr{H}$），它包含了定理C中所述的函数。"允许函数"的确切定义需要引述一些复变函数论中的概念，在此不再细述。对于组合计数问题的解而言，下面的命



题即足以应用，它指出了一类常见的整函数属于“允许函数”类.

命题 1. 设 $p(z)$ 为实系数多项式，$f(z)$，$g(z)\in\mathscr{H}$，$h(z)$ 为整函数，则有

(i) 若 $e^{p(z)}$ 的幂级数展开式中系数 a_n 对所有充分大的 n 均为正值，则 $e^{p(z)}\in\mathscr{H}$.（特别当 $p(z)$ 具有形式(13)，(14)时，$e^{p(z)}\in\mathscr{H}$.）

(ii) 若 $p(z)$ 的最高次项系数为正，则 $p(z)f(z)\in\mathscr{H}$.

(iii) $e^{f(z)}$，$f(z)g(z)\in\mathscr{H}$.

(iv) 若 $\max\limits_{|z|=r}|h(z)|=O(f(r)^{1-\delta})$，其中 $\delta>0$，则 $h(z)+f(z)\in\mathscr{H}$，特别 $f(z)+p(z)\in\mathscr{H}$；又如当 $p(z)$ 最高次项系数为正时，$p(f(z))\in\mathscr{H}$.

例如对 Bell 数 Y_n 之生成函数 $\exp(e^z-1)$，由 (i) $e^z\in\mathscr{H}$，由 (ii) $e^z-1\in\mathscr{H}$，再由 (iii) $\exp(e^z-1)\in\mathscr{H}$.

对于允许函数类 $\mathscr{H}$，下面的定理成立.

定理 C′. 设 a_n 的指数生成函数 $f(z)=\sum a_nz^n/n!\in\mathscr{H}$，则

$$a_n\sim n!f(r)/(r^n\sqrt{2\pi c(r)}),\tag{21}$$

其中 $r>0$，$c(r)$ 定义为

$$(rd/dr)\log f(r)=n,\ c(r)=(r\,d/dr)^2\log f(r).$$

当 $f(z)=e^{p(z)}$ 时，定理 C′ 即化作定理 C.

例 8. Bell 数 Y_n. 它的指数生成函数 $f(z)=\exp(e^z-1)$ 如前述属于 $\mathscr{H}$，故由定理 C′，注意到 $(r\,d/dr)\log f(r)=re^r=n$，$c(r)=(r\ \ d/dr)^2\log f(r)=n(1+r)\sim nr$，即见

$$Y_n\sim n!(2\pi nr)^{-1/2}\exp(e^r-1)r^{-n}.$$

代入 $n!=\sqrt{2\pi n}\,(n/e)^n$，并应用 (4.2.19) 式的渐近解，即可



将 Y_n 的上述渐近式化至(4.2.20)式形式.

例 9(**半群的幂等元**). 考察由集合 $\{1, 2, \cdots, n\}$ 映入自身的函数之全体 $\mathscr{T}_n$. 此种函数可以用记号 $\lambda = \begin{pmatrix} 1, & 2, & \cdots, & n \\ \lambda(1), & \lambda(2), & \cdots, & \lambda(n) \end{pmatrix}$ 来表示,故每个函数 λ 对应于 1, 2, …, n 的一个可重复的 n-排列,因此 $|\mathscr{T}_n| = n^n$. 在 $\mathscr{T}_n$ 中引入乘法运算:$(\lambda\circ\mu)(k) = \lambda(\mu(k))$,则显然$(\lambda\circ\mu)\circ\alpha = \lambda\circ(\mu\circ\alpha)$,亦即$\circ$运算可以结合,因此 $\mathscr{T}_n$ 关于运算$\circ$构成半群. 记 U_n 为 $\mathscr{T}_n$ 中幂等元的个数. 所谓幂等元系指满足 $\lambda\circ\lambda = \lambda$ 的元. 例如当 $n = 1$ 时,$\mathscr{T}_n = \left\{\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right\}$,此唯一的元显为幂等元,故 $U_1 = 1$;当 $n = 2$ 时,$\mathscr{T}_n = \left\{\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}\right\}$,其中除 $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ 外均为幂等元,故 $U_2 = 3$,同样 $U_3 = 10$ 等. 可以证明 U_n 之指数生成函数为$f(z) = \sum U_n z^n/n! = 1 + z + (3/2!)z^2 + (10/3!)z^3 + \cdots = \exp(ze^z)$. 由命题 1,$f(z) \in \mathscr{H}$,故应用定理 C′,注意$(z\,d/dz)\log f(z) = (z + z^2)e^z$,$(z\,d/dz)^2\log f(z) = (z + 3z^2 + z^3)e^z$,即得 $re^r = n/(1 + r)$,$\exp(re^r) = \exp(n/(1 + r))$ 及

$$U_n \sim \left(\sqrt{\frac{1 + r}{2\pi(1 + 3r + r^2)n}}\right)\frac{n!}{r^n}\exp(n/(1 + r)), \tag{22}$$

其中 r 为方程 $(r + r^2)e^r = n$ 之正解.

由于生成函数有各种类型,上述两种类型的定理远不能穷尽应用中遇见的各种情形. 在一般情形,我们仍须借助于复变函数论方法. 设生成函数 $f(z) = \sum a_n z^n$ 在 $|z| < r$ 中解析,由 Cauchy 积分公式知有



$$a_n = (1/2\pi i)\oint_C (f(z)/z^{n+1})dz,$$

其中闭路 C 位于 $|z| < r$ 中. 选取适当的积分路线,使得在其上某点邻近的积分给出全部积分的主要部分, 然后在该点邻近将 $f(z)$ 代之以更简单的形式,便可得出 a_n 的渐近式. 这种方法是渐近分析中比较适用的方法, 但运用时要求有相当熟练的数学技巧. 为完整起见,下面给出此种称为 Laplace 方法的应用一例,更一般的介绍可见 de Bruijn [41].

定理 D. 设 $h(x_1, \cdots, x_n)$ 在包含原点在内的某个有界区域 Ω 内连续,在 $x = 0$ 处达到绝对最大值 $h(0, \cdots, 0) = 0$, 而在 $x_1 = \cdots = x_n = 0$ 的邻近, $h(x_1, \cdots, x_n)$ 有 Taylor 展式

$$h(x_1, \cdots, x_n) = (-1/2)\sum_{i,j=1}^{n} a_{ij}x_ix_j + o\left(\sum_{i=1}^{n} x_i^2\right) \quad \left(\sum x_i^2 \to 0\right), \tag{23}$$

其中 $a_{ij} = (\partial^2 h/\partial x_i\partial x_j)_{x=0}$, 二次形 $\sum_{i,j=1}^{n} a_{ij}x_ix_j$ 对称正定, 则

$$\int\cdots\int_\Omega \exp(th(x_1, \cdots, x_n))dx_1\cdots dx_n \sim (1/\sqrt{D})(2\pi/t)^{n/2} \quad (t\to\infty), \tag{24}$$

其中 $D = \det(a_{ij})$.

我们以一维情形为例, 简略说明该定理的基本思想. 为此记 $I = (-b, b)$, $I_\varepsilon = (-\varepsilon, \varepsilon)$. 于是

$$\int_I e^{th(x)}dx = \int_{I\setminus I_\varepsilon} e^{th}dx + \int_{I_\varepsilon} e^{th}dx,$$

由设在 $I\setminus I_\varepsilon$ 中 $h(x) \leqslant -c < 0$, 故当 $t\to\infty$ 时, $I\setminus I_\varepsilon$ 部



分的积分可以忽略，而在 I_ε 中，因 $h(x) = -ax^2/2 + o(\varepsilon^2)$，故

$$\int_{I_\varepsilon} e^{th}dx \sim \int_{-\varepsilon}^{\varepsilon} e^{-tax^2}dx \sim \int_{-\infty}^{\infty} e^{-tax^2}dx = \sqrt{2\pi/at}.$$

例 10. 设 s, n 为正整数，求当 s 固定，$n \to \infty$ 时

$$S(s, n) = \sum_{k=0}^{2n} (-1)^{k+n} \binom{2n}{k}^s \tag{25}$$

的渐近值。

易见 $S(s, n)$ 等于乘积

$$(-1)^n(1 + z_1)^{2n}(1 + z_2)^{2n}\cdots$$
$$(1 + z_r)^{2n}(1 - (z_1\cdots z_r)^{-1})^{2n}$$

展开式中 $z_1^0 z_2^0 \cdots z_r^0$ 的系数，其中 $r = s - 1$. 因 $S(1, n) = 0$，故下面假设 $s \geqslant 2$, $r \geqslant 1$. 引用 Cauchy 公式，

$$S(r + 1, n) = (-1)^n(2\pi i)^{-r}\int\cdots\int(1 + z_1)^{2n}\cdots(1 + z_r)^{2n}(1 - (z_1\cdots z_r)^{-1})^{2n}(z_1^{-1}dz_1)\cdots(z_r^{-1}dz_r),$$

积分路径可以取作单位圆 $|z_1| = |z_2| = \cdots = |z_r| = 1$. 作变量代换 $z_j = \exp(2i\varphi_j)$ 得

$$S(r + 1, n) = 2^{2n(r+1)}\pi^{-r}\int_{-\pi/2}^{\pi/2}\cdots\int_{-\pi/2}^{\pi/2} \times (\cos\varphi_1\cdots\cos\varphi_r \sin(\varphi_1 + \cdots + \varphi_r))^{2n}d\varphi_1\cdots d\varphi_r. \tag{26}$$

今记

$$G(\varphi_1, \cdots, \varphi_r) = \cos\varphi_1\cdots\cos\varphi_r \sin(\varphi_1 + \cdots + \varphi_r),$$

注意到 G^2 为变量的偶函数，故

$$S(r + 1, n) = 2^{2n(r+1)}\pi^{-r}2 \times \int\cdots\int_{\Omega} G(\varphi_1, \cdots, \varphi_r)^{2n}d\varphi_1\cdots d\varphi_r, \tag{27}$$



其中 Ω 为 $\{-\pi/2 \leqslant \varphi_i \leqslant \pi/2,\ \ i=1, \cdots, r\} \cap \{\varphi_1+\cdots+\varphi_r>0\}$. 注意到在 Ω 的边界上 $G^{2n}=0$，而在 Ω 的内部 G^{2n} 可取正值，故 G^{2n} 的最大值必在 Ω 内部达到，在该点必有 $\partial G/\partial \varphi_j=0 \quad (j=1, \cdots, r)$. 今

$$\partial G/\partial \varphi_j=(-\operatorname{tg} \varphi_j+\operatorname{ctg}(\varphi_1+\cdots+\varphi_r)) G, \tag{28}$$

故在极值点处 $\operatorname{tg} \varphi_1=\operatorname{tg} \varphi_2=\cdots=\operatorname{tg} \varphi_r$，因 $\varphi_j \in(-\pi/2, \pi/2)$，故 $\varphi_1=\cdots=\varphi_r=\alpha$（$\alpha$ 待定）. 进而 $\operatorname{ctg} r\alpha=\operatorname{tg} \alpha$，故 $\alpha+r\alpha=\pi/2+k\pi$，$k$ 为整数. 换言之 $\alpha=\nu\pi/2s$，ν 为奇整数. 因 $|\alpha|<\pi/2$，故 $|\nu|<s$. 在点 $(\alpha, \cdots, \alpha)$ 处

$$\begin{aligned}
G(\alpha, \cdots, \alpha) &=(\cos \alpha)^r \sin r\alpha \\
&=(\cos \alpha)^r \sin (\pi/2+k\pi-\alpha) \\
&=\pm(\cos \alpha)^s,
\end{aligned}$$

在诸极值点 $\alpha=\nu\pi/2s$ 中，最大值 $\max|G|$ 出现在 $\nu=\pm 1$ 两点，因我们只限于 $\varphi_1+\cdots+\varphi_r>0$ 部分，故达最大值之点 $\alpha=s/2\pi$. 记 $\beta=s/2\pi$，在 $(\beta, \cdots, \beta)$ 之邻近

$$\begin{aligned}
G(\varphi_1, \cdots, \varphi_r)=G(\beta, \cdots, \beta) \exp h(\beta \\
+x_1, \cdots, \beta+x_r),
\end{aligned}$$

其中

$$\begin{aligned}
h(\beta+x_1, \cdots, \beta+x_r)=\log G(\varphi_1, \cdots, \varphi_r) \\
-\log G(\beta, \cdots, \beta).
\end{aligned}$$

因 G 有各阶连续偏导数，在 $x_1=\cdots=x_r=0$ 处 $h(\beta+x_1, \cdots, \beta+x_r)$ 取最大值 $h=0$，故在 $x=0$ 邻近 h 形如(23)式，其中的

$$a_{ij}=(\partial^2/\partial \varphi_i \partial \varphi_j) \log G|_{\varphi_1=\cdots=\varphi_r=\beta},$$

由(28)式

$$\begin{aligned}
(\partial^2/\partial \varphi_i \partial \varphi_j) \log G=\partial/\partial \varphi_i(\operatorname{tg} \varphi_j \\
-\operatorname{ctg}(\varphi_1+\cdots+\varphi_r)) \\
=\delta_{ij}(\cos \varphi_j)^{-2}+(\sin (\varphi_1+\cdots+\varphi_r))^{-2}.
\end{aligned}$$



因在 $\varphi_1 = \cdots = \varphi_r = \beta$ 处，$\sin(\varphi_1 + \cdots + \varphi_r) = \sin(r\pi/2s) = \cos(\pi/2s)$，故

$$a_{ij} = (\delta_{ij} + 1)\cos^{-2}(\pi/2s).$$

由此

$$\sum_{i,j=1}^{r} a_{ij}x_ix_j = (x_1^2 + \cdots + x_r^2) + (x_1 + \cdots + x_r)^2\cos^{-2}\beta$$

为一正定二次形. 又用归纳法易证

$$\det(1 + \delta_{ij})_{r\times r} = r + 1 = s,$$

故 $D = \det(a_{ij}) = s\cos^{-2r}\beta$，因此由定理D可见

$$\begin{aligned} S(s,n) &= 2^{2n(r+1)}\pi^{-r}2\int_{\Omega}\cdots\int G^{2n}d\varphi_1\cdots d\varphi_r \\ &\sim 2^{2n(r+1)}\pi^{-r}2G(\beta,\ \cdots,\ \beta)^{2n} \\ &\quad\times\int_{\Omega'}\cdots\int \exp(2nh(\beta + x_1,\ \cdots,\ \beta + x_r)dx_1\cdots dx_r \\ &\sim 2^{2n(r+1)}\pi^{-r}2(\cos\pi/2s)^{2ns}(2\pi)^{r/2} \\ &\quad\times(s\cos^{-2r}(\pi/2s))^{-1/2}(2n)^{-r/2}, \end{aligned}$$

其中 Ω' 为 $(\beta,\cdots,\beta)$ 的某个邻域. 于是最终得出

$$S(s,\ n) \sim (2\cos(\pi/2s))^{2ns+s-1}2^{2-s}(n\pi)^{(1-s)/2}s^{-1/2} \quad (n\to\infty). \tag{29}$$

作为此式的验证,取 $s = 3$ 即得

$$S(3,\ n) \sim 3^{3n+1/2}(2\pi n)^{-1},$$

而由 Dixon 公式(见(3.5.6)式), $S(3,\ n) = (3n)!/(n!)^3$, 应用 Stirling 公式便见 $S(3,\ n)$ 之渐近式确如上述.

4.3.3. 生成函数以隐函数形式给出的情形

在图论计数问题中，生成函数 $w = f(z)$ 常以隐函数 $F(z,\ w) = 0$ 的形式给出,从这种函数方程出发来推求 $f(z)$



的展开式中系数 a_n 之渐近式一般相当困难. 在一些简单情形,可从 $F(z, w) = 0$ 中解出 $w = f(z)$, 例如2.2节中二元树之计数问题. 在另一种特殊情形, $F(z, w) = z - w/\varphi(w)$,亦即 $z = w/\varphi(w)$, 此时若 $\varphi(w)$ 在原点邻近解析且 $\varphi(0) \neq 0$, 则由 Lagrange 反函数展开定理(如见 Фихтенгольц [64]) 可得出 $f(z)$ 的幂级数展开式如下:

$$f(z) = \sum a_n z^n,$$
$$a_n = ((d/dw)^{n-1}\varphi(w)^n)_{w=0}/n!. \tag{30}$$

由此便可进而定出 a_n 的渐近式.

例 11 (**有编号树之计数**). 以 $\tilde{t}_p$ 表示由 p 个有编号顶点构成的树(简称为 p 阶有编号树)的个数. 有如图所示 $\tilde{t}_1 = 1, \tilde{t}_2 = 1, \tilde{t}_3 = 3, \tilde{t}_4 = 16$. 图中数 l 表示该图形的各种不等价编号方式的个数. (两种编号方式 L_1 与 L_2, 若存在顶点的一一对应,使得相邻的点对应于相邻的点,且对应的点编号相同,则称 L_1 与 L_2 等价,例如图 2 所示的两种编号方式即等价.)

图 1 所示的树又称"自由树"或"无根树". 若取此种树中某一点为"根点", 以区别于其它点时, 相应的图称作 "有根

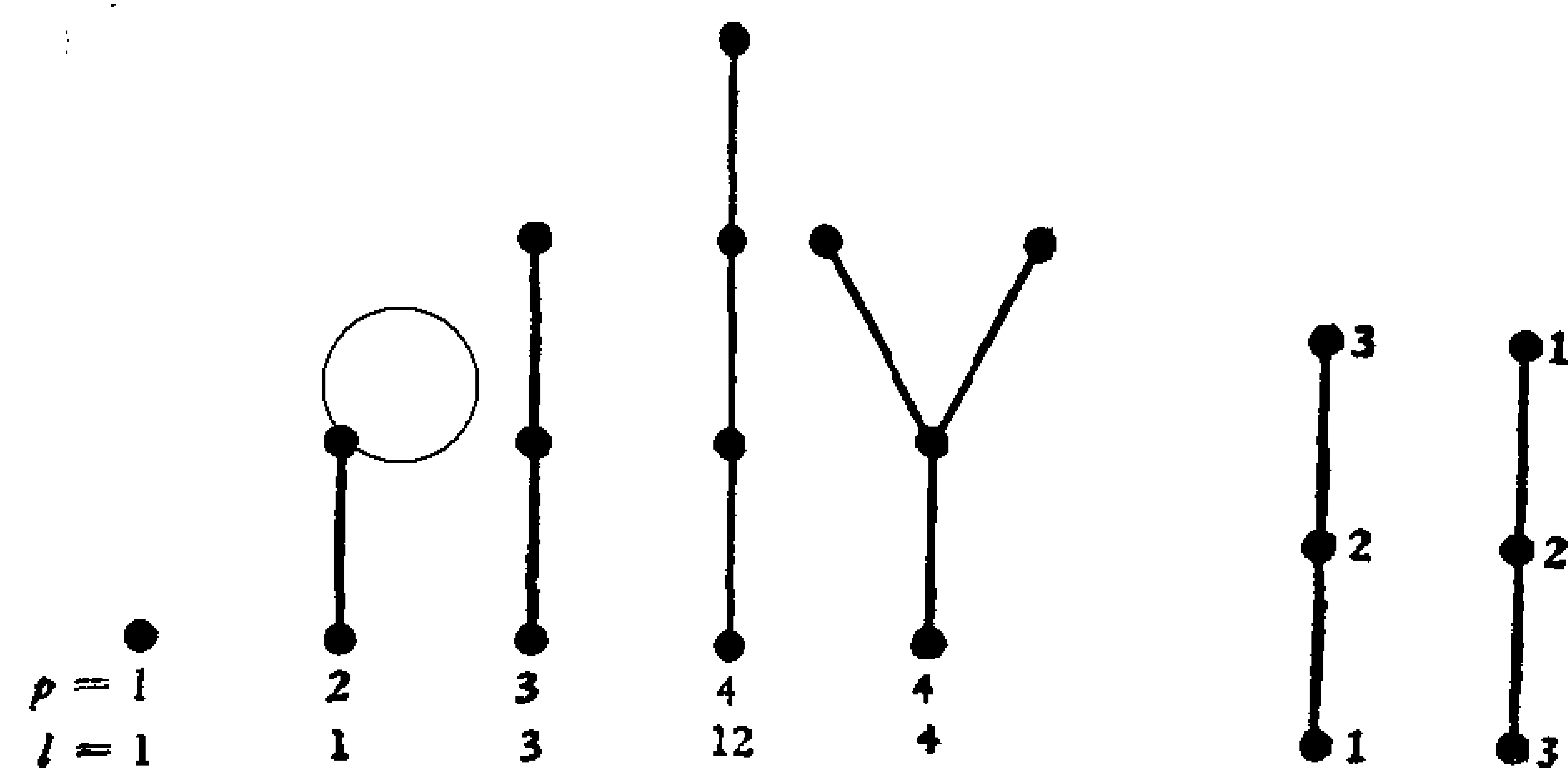


图 1. p 阶有编号树的个数　　　图 2. 两种等价的编号方式



树". 例如与图 1 相应的有根有编号树的个数如图 3 所示(根点用⊙表示)。 每种图形下面的 l 仍表示不等价的编号方式个数。(有根树编号方式的等价性定义与前相仿，只须加上条件：根点与根点相对应。) 若以 t_p 表示 p 阶有根有编号树的个数，则显然 $t_p = p\tilde{t}_p$，此因无根树中每一点均可选作根点。设 t_p 的指数生成函数为

$$w = \sum t_p z^p / p!,$$

Pólya 证得 (见 Harary and Palmer [79])，w 满足函数方程

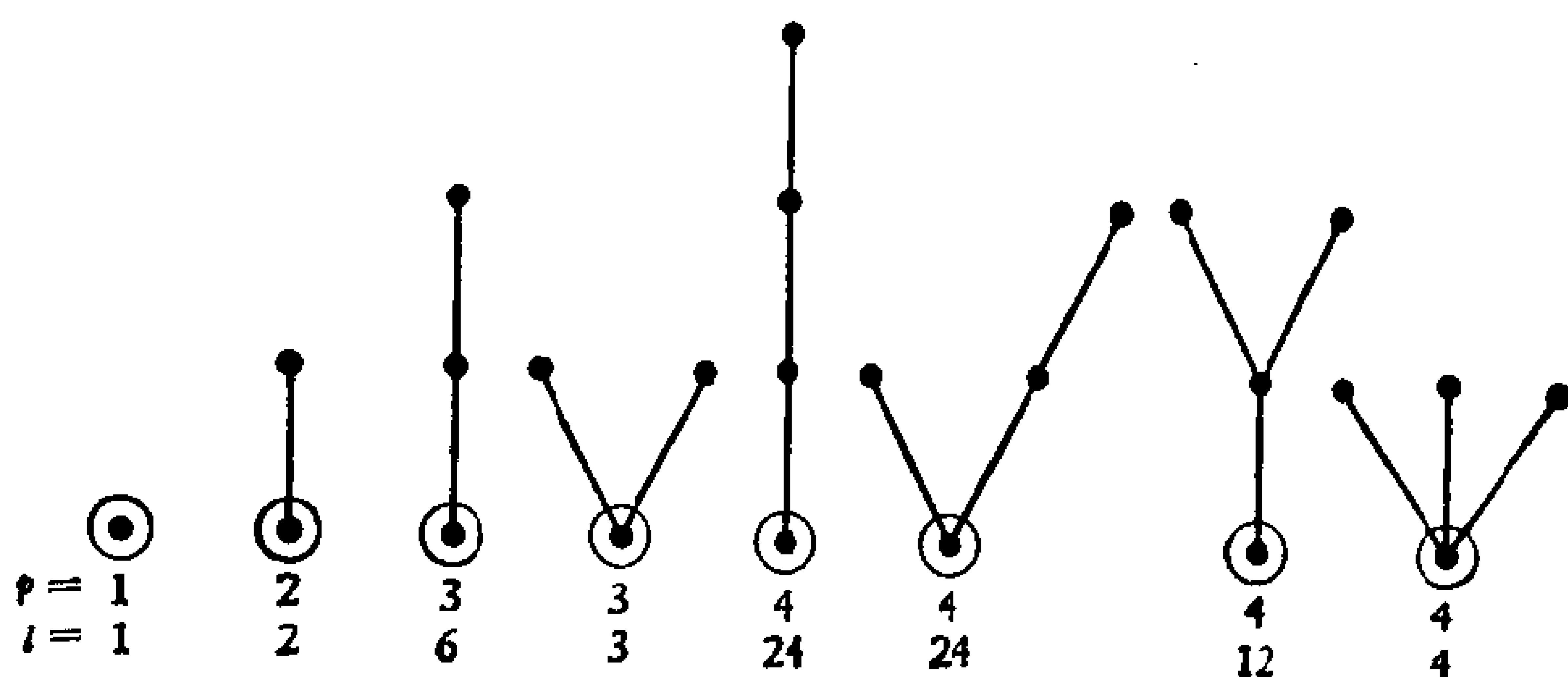


图 3. p 阶有根有编号树的个数

$w = ze^w$ 或 $z = we^{-w}$，于是由 Lagrange 公式(30)得

$$w = \sum_p a_p z^p,$$

$$a_p = ((d/dw)^{p-1}(e^{pw}))_{w=0}/p! = p^{p-1}/p!.$$

因此 $t_p = p^{p-1}$，从而

$$\tilde{t}_p = p^{p-2}, \tag{31}$$

此式本身即可为渐近式。

然而在大多数情形，要由函数方程 $F(z, w) = 0$ 解出 $w = f(z)$ 是十分困难的，我们只能由分析学中的隐函数定理确信在某种条件下此种解的存在性。 为了从 $F(z, w) = 0$ 出发求出 $f(z)$ 的展开式中系数 a_n 的渐近式，我们注意到 a_n 的渐近式常由 $f(z)$ 的奇点性质决定，而由隐函数定理，



$f(z)$ 的奇点又常由 $\partial F/\partial w=0$ 的点 (z, w) 决定,因而我们可以尝试从分析 $\partial F/\partial w=0$ 入手来求得 a_n 的渐近式. 下面的定理见 Harary and Palmer [79].

定理 E. 若生成函数 $w=f(z)=\sum_{n=0}^{\infty} a_n z^n$ 在 $|z|<|z_0|=x_0$ 中解析,而 z_0 为收敛圆上的唯一奇点,在该点级数收敛 $w_0=\sum a_n z_0^n$. 又 w 满足方程 $F(z, w)=0$, 并设 (i) $F(z_0, w_0)=0$; (ii) $(\partial F/\partial w)_{(z_0,w_0)}=0$, $(\partial^2 F/\partial w^2)_{(z_0,w_0)} \neq 0$, 则 $w=f(z)$ 在 z_0 邻近可展成

$$f(z)=f(z_0)+\sum_{k=1}^{\infty} b_k (z_0-z)^{k/2}.$$

而当 $b_1 \neq 0$ 时,

$$a_n \sim (-b_1/2\sqrt{\pi})x_0^{-n+1/2} n^{-3/2}, \qquad (32)$$

若 $b_1=0$, 但 $b_3 \neq 0$ 则

$$a_n \sim (3b_3/4\sqrt{\pi})x_0^{-n+3/2} n^{-5/2}. \qquad (33)$$

例 12 (**无编号有根树的计数**). 以 T_p 表示 p 阶有根的无编号树个数. 由图 3 可见, $T_1=T_2=1$, $T_3=2$, $T_4=4$, 因此时图 3 中每一种图形的 l 种编号方式均相应于一个无编号树. Harary and Palmer 在 [79] 中证得, T_p 的生成函数 $T(z)=\sum T_p z^p$ 满足函数方程

$$T(z)=z\exp\left\{\sum_{k=1}^{\infty} T(z^k)/k\right\}, \qquad (34)$$

故若记 $w=T(z)$, 则

$$F(z, w)=z\left\{\exp\left(w+\sum_{k=2}^{\infty} T(z^k)/k\right)\right\}-w. \qquad (35)$$

Harary and Palmer 在[79]中还证得幂级数 $T(z)=\sum T_p z^p$ 在 $|z|<\eta$ 内收敛,其中 $\eta \geq 1/4$, 且 $T(\eta)=1$. 对(35)式关于 w 求导可得



$$\partial F/\partial w = F(z, w) + w - 1, \tag{36}$$

故 $F'_w(z_0, w_0) = 0$，其中 $z_0 = \eta$，$w_0 = T(\eta) = 1$. 对(36)式关于w再次求导可得

$$(\partial^2 F/\partial w^2)_{(z_0, w_0)} = 1 \neq 0,$$

故定理 E 的条件满足，于是若

$$T(z) = 1 + b_1(\eta - z)^{1/2} + b_2(\eta - z) + b_3(\eta - z)^{3/2} + \cdots,$$

则由(32)式

$$T_p \sim (-b_1/2\sqrt{\pi})\eta^{-p+1/2}p^{-3/2}.$$

Otter 证得

$$b_1\eta^{1/2}/2\sqrt{\pi} = 0.4399237\cdots\cdots,$$

从而

$$T_p \sim 0.4399237\eta^{-p}p^{-3/2}.$$

应用相仿的推理，由 (33) 式可以得出无根无编号的 p 阶树个数 $\tilde{T}_p$ 为

$$\tilde{T}_p \sim 0.5349485\eta^{-p}p^{-5/2}.$$

定理 E 要求我们对 $w = f(z) = \sum a_n z^n$ 的性质有足够多的了解，下面的定理（见 Bender [33]）则减弱了这方面的要求.

定理 F. 设 $w = f(z) = \sum a_n z^n$ 具非负系数，满足 $F(z, w) = 0$，又设存在实数 $r > 0$ 及 $s > a_0$，使得

(i) 对于某个 $\delta > 0$，$F(z, w)$ 在 $|z| < r + \delta$，$|w| < s + \delta$ 中解析；(ii) $F(s, r) = F'_w(r, s) = 0$；(iii) $F'_z(r, s)$，$F''_{w^2}(r, s)$ 不等于零；(iv) 在 $|z| \leqslant r$，$|w| \leqslant s$ 中若 $F(z, w) = F'_w(z, w) = 0$，则 $z = r$，$w = s$，则

$$a_n \sim (F'_z/(2\pi F''_{w^2}))^{1/2} r^{-n+1/2} n^{-3/2}, \tag{37}$$

其中 F'_z 及 F''_{w^2} 在 $z = r$ 及 $w = s$ 处计值.



上述条件 (iv) 因较难验证，可用下面一组条件来代替：

(iv)′ 对充分大的 n，$a_n>0$；(v)′ 存在函数 $\varphi(z, w)$，它在 $|z|<r+\delta$ 及 $|w|<s+\delta$ 中解析，且 (a) 存在某个 $c>0$，使得凡 $F(z, w)=F'_w(z, w)=0$，必有 $\varphi(z, w)=C$；(b) φ 在原点邻近展开的 Taylor 级数有非负系数；(c) 若 φ 与 w 无关，则上述的 Taylor 级数中实际出现的 z 的诸幂次间最大公因数为 1。

例 13 (**凸多边形的剖分**)．给出 $S\subset\{3, 4, 5, 6, 7\cdots\}$．考察将一个凸 n 边形用互不相交的对角线将之剖分的各种方式个数 $d_n(S)$．这里要求剖分后得到的多个多边形之边数属于 S．当 $S=\{3\}$ 时，$d_n(S)$ 即 Cantalan 数 b_{n-2} (见 (2.2.10)式)．例如对 $n=4$，由图 4 见 $d_4=b_2=2$．在一般情形，约记 $d_0(S)=d_1(S)=0$，$d_2(S)=1$，则可以证明 $d_n(S)$ 的寻常生成函数 $D(z, S)=\sum_{n=0}^{\infty} d_n(S)z^n$ 满足方程

$$D(z, S)/z=z+\sum_{k\in S}(D(z, S)/z)^{k-1}. \qquad (38)$$

设诸数 $\{k-2|k\in S\}$ 的最大公因数为 C，易证若 $n-2$ 非 C 的倍数，则 $d_n(S)=0$，而当 $n-2$ 为 C 的倍数时，则对充分大的 n，$d_n(S)>0$．今首先考察 $C=1$ 的简单情形．为应用定理 F，置 $w(z)=D(z, S)/z$，于是

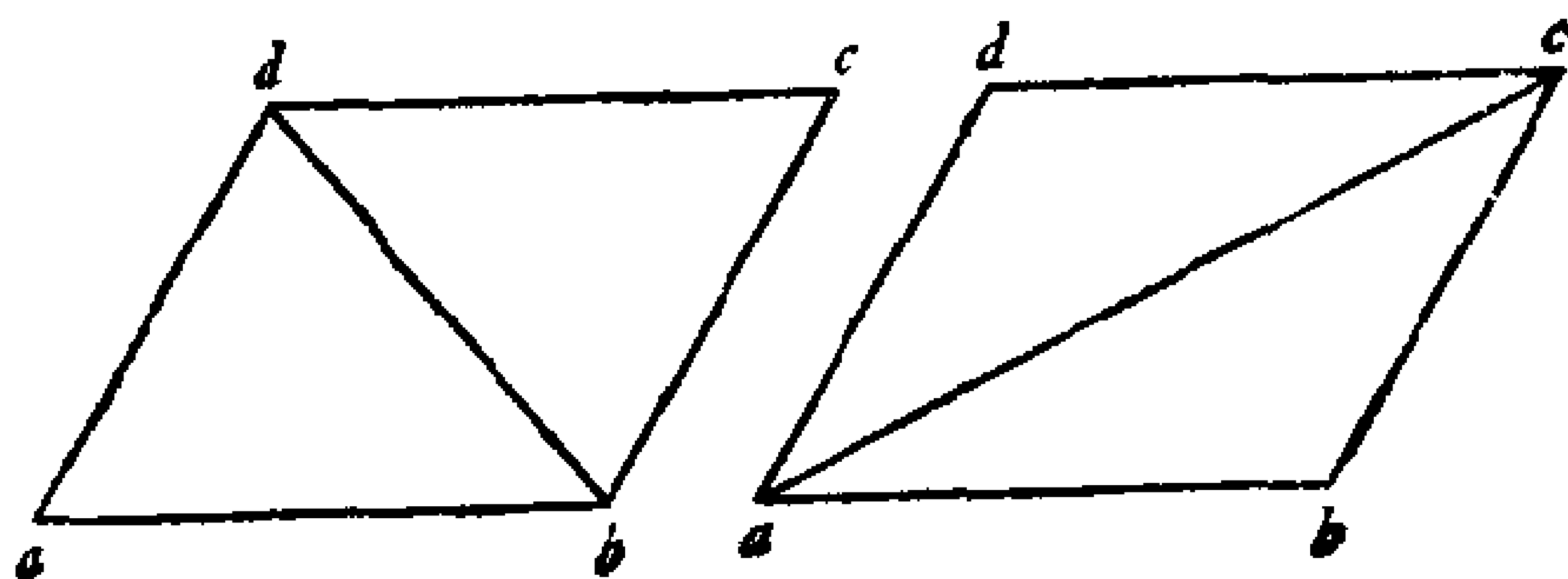


图 4． 凸四边形剖分成三角形



$$F(z, w) = z - w + \sum_{k \in S} w^{k-1}. \qquad (39)$$

显然 F 在 $|w| < 1$ 中解析，又

$$F'_w = -1 + \sum_{k \in S} (k-1) w^{k-2}, \qquad (40)$$

易见 $F'_w = 0$ 有唯一的正解 $w = s < 1$，将 s 代入(38)即可定出 $z = r$，于是定理F中的条件 (i) 与 (ii) 满足；由 F 的表示式(39)易验条件 (iii) 满足；又由 $C = 1$ 知 (iv)′ 满足。而条件 (v)′ 中的 $\varphi(z, w)$ 可取作(40)式中的和式 $\sum_{k \in S}(k-1)w^{k-2}$，此时 (v)′ 中诸条件显然满足，故由定理F，

$$d_n(S) = a_{n-1} \sim (1/2\pi F''_{w^2})^{1/2} n^{-3/2} r^{3/2-n},$$

其中

$$F''_{w^2} = \sum_{k \in S} (k-1)(k-2) s^{k-3},$$

$$r = s - \sum_{k \in S} s^{k-1},$$

s 为 $\sum_{k \in S} (k-1) w^{k-2} = 1$ 之唯一正根。

当 $\{k - 2 | k \in S\}$ 之最大公约数 $C > 1$ 时，可作代换 $\tilde{z} = z^C$，并取 $w = D(z, S)/z^2$ 经相仿的推理即可得在此一般情形

$$d_n(S) \sim C(1/2\pi F''_{w^2})^{1/2} n^{-3/2} r^{3/2-n}.$$

今考察两个极端情形：(i) 当只允许剖分成三角形时，$S = \{3\}$，$C = 1$，而 $F = z - w + w^2$，由此易见 $s = 1/2$，$r = 1/4$，$F''_{w^2} = 2$，故

$$d_n \sim (\pi n^3)^{-1/2} 4^{n-2}, \qquad (41)$$

此与精确公式

$$d_n = b_{n-2} = \binom{2n-4}{n-2} \Big/ (n-1)$$



相符(比较(4.2.7)式).

(ii) $S=\{3, 4, 5, \cdots\}$, 即剖分后的多边形边数不限. 此时 $C=1$, $F=z-w+\sum_{k=2}^{\infty} w^k=z-w+w^2/(1-w)$. 由此易解出 $s=(2-\sqrt{2})/2$, $r=3-\sqrt{2}$, $F''_{w^2}=4\sqrt{2}$, 从而

$$d_n \sim ((3\sqrt{2}-4)/n\pi)^{1/2}(3+2\sqrt{2})^{n-1}/4n.$$

Bender 在[33]中还给出了定理 F 在有根及无根无编号二元树之计数问题的应用例子,限于篇幅,此处不再引述了.

4.4. 渐近式的直接推导例: 拉丁矩阵的计数

在上两节中我们给出了当计数问题的解以和式或生成函数形式表出时,渐近式的推导方法,但由于组合计数问题的多样性和复杂性,有许多计数问题,迄今仍得不到它的明显表示式[1]. 在这些场合,我们便需要从问题的要求出发直接推导它的渐近式. 关于渐近式的直接推求方法,由于问题的多样性,当无一般模式可循,无非是估计解的上下限,并证明其差为高阶小量. 本节将以拉丁矩阵的渐近计数为例作为直接推导渐近式的一个说明性例子.

所谓 k 行 n 列 $(k\times n)$ 的拉丁矩阵系指数字 1 至 n 组

---

1) 这里,要严格地说明什么样的表示式可称得上是"明显表示式"是很困难的. 例如以数论中的 $\pi(x)$ 为例, $\pi(x)$ 表示不超过 x 的素数个数,由定义便可写出 $\pi(x)=\sum_{p\leqslant x} 1$, 其中和式遍及不超过 x 的所有素数 p. 若引用一些数论函数,还可写出 $\pi(x)$ 的更精细的表示式. 尽管如此,我们并不认为这些表示式是"明显表示式". 因在我们看来,像 $\pi(x)=\sum_{p\leqslant x} 1$ 一类的表示式只不过是将 $\pi(x)$ 用文字语言叙述的定义改用符号语言写出来而已.



成的阵，其中每行每列都无重复的元，亦即每行为 $\{1, 2, \cdots, n\}$ 的一个 n-排列，每列为 $\{1, 2, \cdots, n\}$ 的一个 k-排列. $k \times n$ 的拉丁矩阵的个数记作 $L(k, n)$. 关于 $L(k, n)$ 的明显表示式，迄今只解决了 $k \leqslant 3$ 的情形，Light 在[102]中提出了计算 $L(4, n)$ 的一种方法. 由于 $L(k, n)$ 一般表式难于求出，人们便尝试直接推求 $L(k, n)$ 的渐近式. Erdős and Kaplamsky 在[58]中得到了第一个重要结果，证得：若 $k < (\log n)^{3/2-\varepsilon}$，则

$$L(k, n) \sim (n!)^k \exp\left(-\binom{k}{2}\right). \tag{1}$$

他们并猜测这一渐近式的有效性可扩充到 $k < n^{1/3-\varepsilon}$ 的情形. 其后，1951 年，Yamamoto 证明了这一猜测（见 Ryser [139]）. 下面我们着手证明 Erdös and Kaplansky 的结果(1).

假设 L 为任意给定的一个 k 行 n 列的拉丁阵：$L = (a(i, j))_{k\times n}$. 我们考察在 L 中添加第 $k+1$ 行，使之成为 $(k+1)\times n$ 拉丁阵的不同方式个数 N. 首先，第 $k+1$ 行须从 $n!$ 个排列构成的集合 $\sum_n$ 中选取. 为了求得 $\sum_n$ 中可选为第 $k+1$ 行的排列个数，我们应用入与出原理如下：一个排列 σ 若具有

$$\sigma(j) = a(i, j), \tag{2}$$

其中 $1 \leqslant i \leqslant k$，则称 σ 具有性质 P_{ij}. 显然不具有任一性质 P_{ij} 的排列都可选为第 $k+1$ 行. 于是由定理(3.4.A)，

$$N = P_=(0) = \sum_{r=1}^{n} (-1)^r S_r,$$

其中 S_r 为至少满足 r 个形如(2)式的排列个数. 今从阵 L 的不同列中任取 r 个互异的数

$$a(i_1, j_1), a(i_2, j_2), \cdots, a(i_r, j_r), \tag{3}$$



其中 $1 \leqslant i_p \leqslant k$，$j_1 < j_2 < \cdots < j_r$. 显然，满足 $\sigma(j_p) = a(i_p, j_p)$ $(p = 1, \cdots, r)$ 的排列个数有 $(n-r)!$ 个，因此若形如(3)的数组有 A_r 个，则 $S_r = (n-r)!A_r$，即

$$N = \sum_{r=1}^{n} (-1)^r (n-r)! A_r. \tag{4}$$

对于数 A_r 本身我们再次使用入与出原理. 形如 (3) 但不要求 $a(i_p, j_p)$ 间互异的数组共有 $\binom{n}{r} k^r$ 个，此因 $j_1 < j_2 < \cdots < j_r$ 有 $\binom{n}{r}$ 种取法，而每个 i_p 有 k 种取法. 因此，若

$$a(i_p, j_p) = a(i_q, j_q) \qquad (p < q), \tag{5}$$

时称数组 (3) 具有性质 P_{pq}，则 A_r 即为此种性质集合下的 $P_=(0)$，故

$$A_r = \sum_{s} (-1)^s B_s(r), \tag{6}$$

其中 $B_s(r)$ 为至少满足 s 个形如 (5) 式的数组 (3). 特别 $B_0(r)$ 即为形如(3) $(j_1 < \cdots < j_r)$ 的数组个数，故由上述

$$B_0(r) = \binom{n}{r} k^r. \tag{7}$$

对于 $B_1(r)$，即至少对于一对 $p < q$，(5)式成立的数组(3)之个数，可讨论如下：首先注意到若 $a(i_p, j_p) = a(i_q, j_q)$，则 $i_p \neq i_q$，故 (i_p, i_q) 共有 $\binom{k}{2}$ 种取法，(i_p, i_q) 取定后值 $a(i_p, j_p) = a(i_q, j_q) = u$ 有 n 种取法. 又(3)中剩下的 $r-2$ 个元计有 $\binom{n-2}{r-2} k^{r-2}$ 种取法，因此

$$B_1(r) = n \binom{k}{2} \binom{n-2}{r-2} k^{r-2}.$$



对于 $B_2(r)$，即至少满足两个形如(5)式的数组(3)个数，则需作更细致的讨论．试比较 $a=b$, $c=d$ 与 $a=b$, $b=c$，每组都由两个等式组成，但前者涉及到四个元 a, b, c, d，后者只涉及到三个元 a, b, c．在前一情形所述的二个等式涉及到分布在四个不同列中的元，于是剩下的元共有 $\binom{n-4}{r-4}k^{r-4}$ 种取法；在后一情形，二个等式只涉及到三个不同列中的元，剩下的元共有 $\binom{n-3}{r-3}k^{r-3}$ 种取法．一般说来，若 s 个形如(5)的等式计涉及到 t 个不同列中的元，则剩下的 $r-t$ 个元即有 $\binom{n-t}{r-t}k^{r-t}$ 种取法．因此，若从阵 L 的 t 个不同列中选出 t 个元，使得它们间共成立 s 个等式，若此种 t 个元有 $F(s, t)$ 种取法，则

$$B_s(r)=\sum_t F(s, t)\binom{n-t}{r-t}k^{r-t}. \tag{8}$$

这里应注意 t 的变动范围，在最多时可达 $t=2s$（如 $a=b$, $c=d$, $t=4=2s$）；在最少时可能成立 $\binom{t}{2}=s$ $\Big($如 $a=b$, $b=c$, $t=3, s=\binom{3}{2}=3\Big)$．故(8)式中和式变量 t 变动于 $s\leqslant\binom{t}{2}$ 及 $t\leqslant 2s$ 之间．今证

引理 1. $$\sum_s F(s, t)<n^{t/2}(k^2t)^{t^2}. \tag{9}$$

实际上，$\sum_s F(s, t)$ 给出了下述选取方式的总数：从 L 的 t 个不同列中选出 t 个元来，使得它们之间有为数不限的



若干组形如(5)的等式成立．为了估计这种选取方式的个数，我们首先注意到这 t 个元相互间需要配对，因而至多包含了 $[t/2]$ 个不同的整数（例如 $a=b$, $c=d$ 只包含了二个整数）．由此可见，组成这 t 个元的不同整数共有 $\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{[t/2]}\leqslant n^{t/2}$ 种选取方式． t 个元一旦确定，至多形成 $\binom{t}{2}<t^2$ 个等式．每个等式 $a=b$ 至多有 $\binom{k}{2}t/2$ 种方式表现为阵 L 中的一对相等的元，亦即 a 与 b 所在行有 $\binom{k}{2}$ 种选法，值 $u=a=b$ 有 $t/2$ 种选法．任意选定的 s 个等式不过是这 $\leqslant t^2$ 个等式在阵 L 的一种"放法"．因此 t 个元一经确定，至多有 $\left(\binom{k}{2}t/2\right)^{t^2}\leqslant(k^2t)^{t^2}$ 种"放法"，由此即得(9)式。

定理 A. 若 $k<(\log n)^{3/2-\varepsilon}$，其中 ε 为任意正数，则对充分大的 n

$$|(Ne^k/n!)-1|<n^{-c} \tag{10}$$

成立，其中 c 为仅与 ε 有关的正常数。

证． 记 $m=[(\log n)^{1-\varepsilon}]$，并置

$$A(r,m)=\sum_{s=1}^{m-1}(-1)^s B_s(r), \tag{11}$$

于是由(4)及(6)式

$$N=\sum_r(-1)^r(n-r)!A_r$$

$$=\sum_r(-1)^r(n-r)!(A_r-B_0(r)$$



$$- A(r, m)) + \sum_r (-1)^r (n-r)! B_0(r)$$

$$+ \sum_r (-1)^r (n-r)! A(r, m).$$

由 Bonferroni 不等式(见(4.2.21)式)知

$$|A_r - B_0(r) - A(r, m)| \leqslant B_m(r),$$

故代入 $B_0(r) = \binom{n}{r} k^r$ 可见

$$\left| N - \sum_r (-1)^r (n-r)! \binom{n}{r} k^r \right| \leqslant |G| + H, \quad (12)$$

其中

$$G = \sum_{r=0}^{n} (-1)^r (n-r)! A(r, m),$$

$$H = \sum_{r=0}^{n} (n-r)! B_m(r). \quad (13)$$

对于和式 G,由(8)及(11)式,

$$G/n! = \sum_{r=0}^{n} ((-1)^r (n-r)!/n!)$$

$$\times \sum_{s=1}^{m-1} (-1)^s \sum_t F(s, t) \binom{n-t}{r-t} k^{r-t}$$

$$= \sum_{s=1}^{m-1} (-1)^s \sum_t F(s, t)$$

$$\times \sum_{r=t}^{n} (-1)^r \binom{n-t}{r-t} k^{r-t} \Big/ [n]_r.$$

作变量代换 $u = r - t$,

$$\sum_{r=t}^{n} (-1)^r \binom{n-t}{r-t} k^{r-t} \Big/ [n]_r$$



$$= ((-1)^t/[n]_t) \sum_{u=0}^{n-t} (-k)^u/u!$$

$$= (-1)^t(e^{-k} - \theta)/[n]_t,$$

式中 θ 为将 e^{-k} 展开到 $(n-t)$ 项后的余项。因而

$$|G|e^k/n! \leqslant \sum_{s=1}^{m-1} \sum_t F(s, t)(1 + \theta e^k)/[n]_t. \quad (14)$$

如前所述，t 的变动范围不超出 $[\sqrt{s}, 2s]$，故 $t \leqslant 2s < 2m < 2\log n$。由此易见

$$1/[n]_t < c_1 n^{-t}, \quad (15)$$

$$\theta e^k < c_2. \quad (16)$$

再由(8)式即见

$$|G|e^k/n! < c_3 \sum_{t=1}^{2m} (k^2 t)^{t^2}/n^{t/2},$$

其中 $c_3 = c_1(1 + c_2)$。今 $t \leqslant 2m < 2(\log n)^{1-\varepsilon}$，故易见 $(k^2 t)^{t^2}$ 之对数等于 $O(t^2 \log\log n)$，而 $n^{t/2}$ 之对数等于 $O(t \log n)$，因此对于充分大的 n

$$(k^2 t)^{t^2}/n^{t/2} < n^{-c_4},$$

从而

$$|G|e^k/n! < 2mc_3 n^{-c_4} < n^{-c_5}, \quad (17)$$

其中 c_4 及 c_5 均为仅与 ε 有关的正常数。

下面转而考察(13)式所确定的 H，由(8)式

$$H/n! = \sum_{r=0}^{n} \sum_t F(m, t) \binom{n-t}{r-t} k^{r-t}/n!$$

$$= \sum_t F(m, t) \sum_{r=t}^{n} \binom{n-t}{r-t} k^{r-t}/n!.$$

如前所证，后一和式为构成 e^k 的 Taylor 展式之前 $n-t$ 项与 $1/[n]_t$ 之积，故



$$H/n! < e^k \sum_t F(m, t)/[n]_t$$

$$< c_1 e^k \sum_t (k^2 t)^{t^2}/n^{t/2}.$$

注意到此时求和下标 t 的起始值为$\sqrt{m} > c_6(\log n)^{(1-\varepsilon)/2}$，故 $(t/2)\log n \geqslant c_6(\log n)^{3/2-\varepsilon/2}$. 因 $\log e^{2k} = 2k < 2(\log n)^{3/2-\varepsilon}$，故对充分大的 n

$$e^{2k}(k^2 t)^{t^2}/n^{t/2} < n^{-c_7},$$

从而

$$He^k/n! < 2mc_1 n^{-c_7} < n^{-c_8}.$$

由此式及(12),(17)式即证得(10)式.

由定理A立即可以推出

定理 B. 对于 $k < (\log n)^{3/2-\varepsilon}$,有

$$L(n, k) \sim (n!)^k e^{-\binom{k}{2}}.$$

证. 由定理A可见，$L(n, i+1)$ 之值介于 $L(n, i)n! \times e^{-i}(1 \pm n^{-c})$ 之间，令 i 从1增至 $k-1$，并相乘即见 $L(n, k)$ 之值介于 $(n!)^k e^{-\binom{k}{2}}(1 \pm n^{-c})^k$ 之间,但 $(1 \pm n^{-c})^k \sim 1$,即证得本定理.

我们曾在3.5节中指出：将一个 $k \times n$ 的拉丁阵扩充成 $(k+1) \times n$ 的拉丁阵的各种方式个数等于一个 $U(n, n-k)$ 类(0,1)矩阵之常值,由此易见,定理B可以等价地叙述为

定理 B′. 若 $A \in U(n, n-k)$, $k < (\log n)^{3/2-\varepsilon}$, 则

$$\operatorname{Per}(A) \sim n! e^{-k}. \tag{18}$$

由 Yamamoto 所获的结果，上述定理的适用范围可扩大到 $k < n^{1/3-\varepsilon}$. 为了估计更大范围中的 $L(n, k)$ 值，我们注意到由 van der Waerden 猜测（见(3.5.7)式）可见，对 $A \in U(n, n-k)$ 有

$$\operatorname{Per}(A) \geqslant (1 - k/n)^n n!,$$



由此将可引出

$$
\begin{aligned}
L(n, k) \geqslant (1 - 1/n)^n (1 &- 2/n)^n \cdots \left(1 - \frac{k-1}{n}\right)^n (n!)^k \\
&= ([n]_k / n^k)^n (n!)^k. \qquad (19)
\end{aligned}
$$

当 $k < n^{1/3-\varepsilon}$ 时,上式右边 $\sim (n!)^k \exp\left(-\binom{k}{2}\right)$(而当 $k \geqslant n^{1/3}$ 时便不再成立),故我们猜测:对更大范围内的 k 值将有

$$
L(n, k) \sim ([n]_k / n^k)^n (n!)^k. \qquad (20)
$$

又由(3.5.10)式可得,若 van der Waerden 猜测为真,则

$$
(n!)^{2/n}/n \leqslant L(n, n)^{1/n^2} \leqslant \left(\prod_{k=1}^{n-1} (k!)^{1/k}\right)^{1/n}.
$$

应用 Stirling 公式易证,上式两边均 $\sim ne^{-2}$,由此引出 O'Neil [121] 中的一个猜测:

$$
(L(n, n))^{1/n^2} \sim ne^{-2}. \qquad (21)
$$

两个猜测(20)及(21)迄今均未得到证明。



第五章　群论方法的应用

5.1. 置换群和等价类

在分放问题（将 m 个球放入 r 个盒子中）、图论计数问题等一些组合计数问题中，我们常需说明球、盒子、图的顶点等计数对象是有编号的，还是无编号的？或者说是有区别的，还是无区别的？ 这是两类具有根本差别的计数问题．一般来说，无编号的计数问题比有编号的计数问题要困难得多，其间原因可用下面的简单例子予以说明．

例 1.　考察图 1 所示的树形图 S，问用两种色 A 和 B 染图 S 的六个顶点共有多少种不同的染法？

情形(i).假定 S 的诸顶点是有编号的，亦即这六个点可以相互区别，此时只要一个点 a_i 在两种染色方式下染以不同

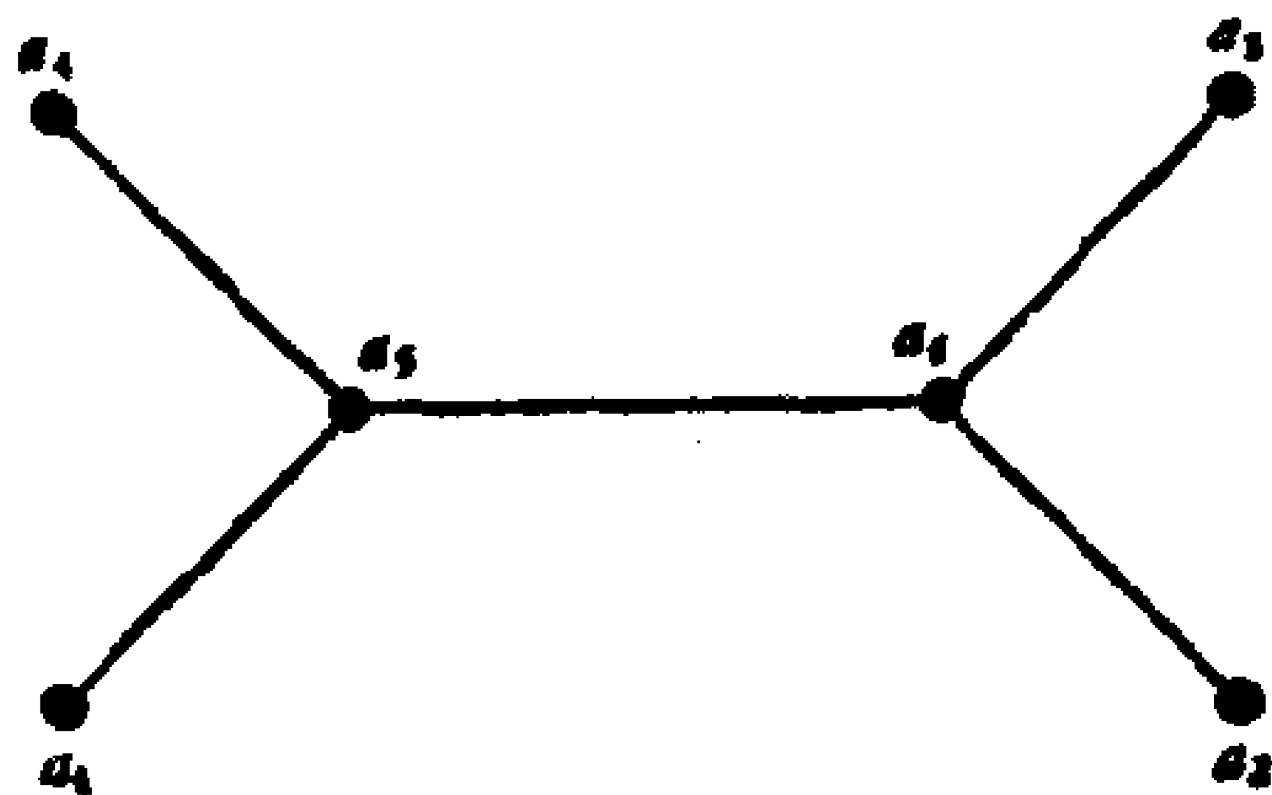


图　1.

的色，便认为这两种染色方式是不同的．故它的求解极为简单：因每个顶点之染色有 2 种选择，而 S 共有六个顶点，故共有 $2^6=64$ 种不同的染色方式．由此可见，在求解时，我们只需知道 S 有 6 个顶点便已足够，至于这些顶点之间是如何连



结的，则不必计较.

情形 (ii). 无编号情形. 此时图 2 所示的两种染色方法便认为是相同的(或者说得更确切些，是等价的)，因若将图 2 左边的图形绕轴 $\overline{a_5a_6}$ 转动 180° 便与右边的图相重合，然而下列两种染色方式 $(a_1a_2\cdots a_6)=(AAAAAA)$ 与 $(AAAABB)$ 则不论

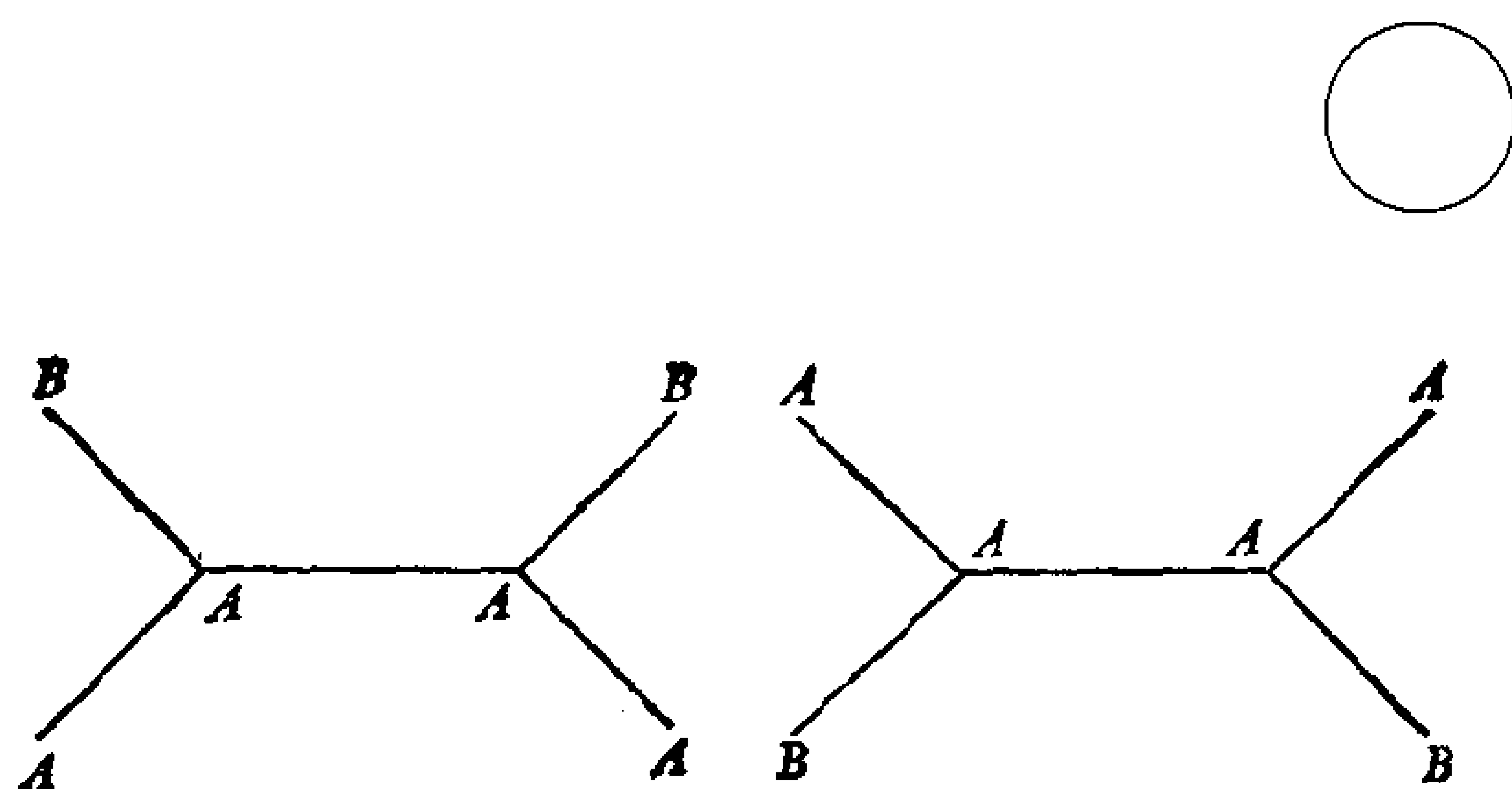


图 2. 两种等价的染色方式

将 S 作何种运动总不会相重，故为两种不等价的染色方式. 因而在无编号情形，求解显得困难得多，不同的染色方式个数与图形结构的"对称"性密切相关. 为了仔细研究这类情形，我们需要引入置换群的若干最基本的概念.

设 $S=\{a_1,\cdots,a_n\}$ 为一有限集合，S 与自身间的一一对应：$a\in S\longleftrightarrow f(a)\in S$，称作集合 S 上的一个置换，每个置换可以写成

$$f=\begin{pmatrix}1 & 2 & 3\cdots n\\ i_1 & i_2 & i_3\cdots i_n\end{pmatrix},$$

它表示函数 f 将 a_1 映成 $f(a_1)=a_{i_1}$，a_2 映成 $f(a_2)=a_{i_2}$，$\cdots$. 既然 f 为一一对应，故当 $a\neq b$ 时，$f(a)\neq f(b)$，由此可见 $(i_1i_2\cdots i_n)$ 为 $\{1,2,\cdots,n\}$ 的一个 n-排列，例如对图 1 所示的图 S，绕轴 $\overline{a_5a_6}$ 旋转 180° 后，a_1 与 a_4，a_2 与 a_3 位置互换，而 a_5 与 a_6 位置不变，故相当于置换



$$g_1=\begin{pmatrix}1&2&3&4&5&6\\4&3&2&1&5&6\end{pmatrix}. \qquad (1)$$

若 f_1, f_2 为两个置换，则其积 f_1f_2 定义为

$$(f_1f_2)(a)=f_1(f_2(a)),\ a\in S, \qquad (2)$$

亦即先施行置换 f_2，再施行 f_1 所得的结果．例如当

$$f_1=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\quad f_2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

时，积

$$f_1f_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\quad f_2f_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}.$$

由此例可见，一般 $f_1f_2\neq f_2f_1$．当 $f_1=f_2$ 时，记 f_1f_1 为 f_1^2，一般记 $f_1^n=f_1f_1\cdots f_1$（n 个 f_1 之积）．此外约定 $f^0=e$，e 为恒等置换：$e(a)=a$．

任取 $a\in S$，考察元列

$$a, f(a), f^2(a), f^3(a), \cdots.$$

由定义，列中每一元都属于 S，但 S 为一有限集，故总可以找到最小的一对数 $p<q$，使得 $f^p(a)=f^q(a)$． 易证 $p=0$．不然，若 $p\geqslant 1$，则由 (p, q) 的最小性，$f^{(p-1)}(a)\neq f^{(q-1)}(a)$，这与置换的定义 $a\neq b\Rightarrow f(a)\neq f(b)$ 相矛盾．因此总可以找到最小的 $l\geqslant 1$，使得 $f^l(a)=a$，而 $a, f(a), \cdots, f^{l-1}(a)$ 互不相同． 得到 $a, f(a), \cdots, f^{l-1}(a)$ 后，我们再从 S 中另取一元 b，用同一推理知存在 $t\geqslant 1$，使得 $b, f(b), f^2(b), \cdots, f^{t-1}(b)$ 互不相同，而 $f^t(b)=b$．如此继续可见，每个置换 f 必可分解成诸"轮换"之积：

$$f=(a, b, c, \cdots, p, q)(r, s, t, \cdots, u, v)\cdots \times(h, l, \cdots, w),$$

其中诸元 $a, b, \cdots, p, q, r, s, \cdots, w$ 互异，形如 $(a, b, c, \cdots, p, q)$ 的因子称作"轮换"，它表示 $f(a)=b, f(b)=$



$c, \cdots, f(p)=q$ 并 $f(q)=a$. 例如置换(1)可以分解成

$$g_1=(1,4)(2,3)(5)(6), \tag{3}$$

其中(5)表示 $g_1(5)=5$. 同样若 g_2 为图 S 关于过 $\overline{a_5a_6}$ 的中点 O 并垂直于它的轴的 $180°$ 旋转,则

$$g_2=(1,2)(3,4)(5,6). \tag{4}$$

而 g_1 与 g_2 之积 $g_3=g_1g_2$ 即为绕 $\overline{a_5a_6}$ 中点 O 的 $180°$ 旋转

$$g_3=(1,3)(2,4)(5,6). \tag{5}$$

若置换 f 可以分解成 b_1 个长为 1 的轮换, b_2 个长为 2 的轮换…之积,则称 f 属于类型 $\{b_1, b_2, \cdots\}$. 例如上述置换 g_1 由 2 个长为 2 的轮换, 2 个长为 1 的轮换之积形成,故属于类型 $\{2,2,0,0,0,0\}$. 由定义可见,若集合 S 有 n 个元,则

$$b_1+2b_2+3b_3+\cdots+nb_n=n.$$

亦即所有轮换因子的长度之和等于集合 S 中元的个数.

记 S_n 为 S 上所有 $n!$ 个置换所构成的集合. 容易验证, S_n 关于(2)式所定义的乘法构成群(群的定义见 3.3 节). 实际上此时单位元 e 即为恒等置换 $e=\begin{pmatrix}1 & 2 & \cdots & n\\ 1 & 2 & \cdots & n\end{pmatrix}$; 而任一 $f=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}$ 之逆元即为 $f^{-1}=\begin{pmatrix}i_1 & i_2 & \cdots & i_n\\ 1 & 2 & \cdots & n\end{pmatrix}$. 例如 $\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix}$ 之逆为 $\begin{pmatrix}2 & 3 & 4 & 1\\ 1 & 2 & 3 & 4\end{pmatrix}$,将其列重排即得 $\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}$. 群 S_n 一般称为 **n 个文字的对称群.**

若 S_n 的一部分置换本身构成一个群 G,则称 G 为 S_n 的子群. 此时常直接称 G 为一置换群. 例如

$$f_1=(1,2)(3,4),\ f_2=(1,3)(2,4),$$
$$f_3=(1,4)(2,3),\ e=(1)(2)(3)(4) \tag{6}$$



所组成的 $G=\{f_1, f_2, f_3, e\}$ 即构成 S_4 的一个子群，此时每个 f_i 之逆为其自身：$f_i^{-1}=f_i$。

设 G 为集合 S 上的一个置换群。对任一属于类型 $\{b_1, b_2, \cdots, b_n\}$ 的置换 $g\in G$，使之与 n 个变量的一个单项式 $x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}$ 相对应，并定义

$$P_G(x_1, x_2, \cdots, x_n)=|G|^{-1}\sum_{g\in G}x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n} \tag{7}$$

称为 G 的轮换指标。

例 2. $G=\{e\}$，亦即群 G 只包含一个恒等置换 $e=(1)(2)\cdots(n)$。此时 $b_1=n, b_i=0\ (i>1)$。故 $P_G=x_1^n$。

例 3. 群(6)。此时 $n=4$，e 属于类型 $\{4, 0, 0, 0\}$，f_1, f_2, f_3 属于 $\{0, 2, 0, 0\}$，故 $P_G=(x_1^4+3x_2^2)/4$。

例 4. 考察图 1 所示的图 S。使得 S 不变的诸旋转构成群 G，它由(3)，(4)，(5)三式所定义的置换连同恒等置换 e 组成，亦即

$$G=\{g_1, g_2, g_3, e\}, \tag{8}$$

它的轮换指标为

$$P_G=(x_1^6+x_2^2x_1^2+2x_2^3)/4. \tag{9}$$

此例中，G 的每个置换都给出了图 S 中各顶点间的一种对称关系。例如置换 g_1 指出点 a_1 与 a_4 对称，a_2 与 a_3 对称；g_2 则指出 a_3 与 a_4 对称…。将这种对称概念推广之，即引出“等价”的概念。

定义 1. 设 G 为 S 上的一个置换群。对于 S 中的两个元 a_1 与 a_2，若存在置换 $g\in G$，使得 $g(a_1)=a_2$，则称 a_1 与 a_2 等价，并记作 $a_1\sim a_2$。

今证上述定义的关系 $\sim$ 满足下述三种性质：

(i)（自反性）$a\sim a$；(ii)（对称性）$a\sim b\Rightarrow b\sim a$；(iii)（传递性）$a\sim b, b\sim c\Rightarrow a\sim c$。 (10)



实际上，对于恒等置换 $e\in G$，有 $e(a)=a$，故 $a\sim a$；又若 $g(a)=b$，则 $g^{-1}(b)=a$，故有 (ii)．最后，$g_1(a)=b$，$g_2(b)=c\Rightarrow(g_2g_1)(a)=c$，即得 (iii)．

一般，集合 S 中诸元间的任一种关系，若满足上述性质 (i)—(iii)，即称为一种等价关系．任一种等价关系必给出集合 S 的一个分划：$S=\bigcup\limits_i S_i$，其中每个 S_i 由彼此等价的元构成．每个 S_i 称为一个等价类．例如例 4 中的图 S 的 6 个点，关于群(8)即划分成两个等价类．下面的重要引理给出了 S 中等价类的个数．

引理 1 (Burside)． 集合 S 的等价类个数等于

$$|G|^{-1}\sum_{g\in G}\phi(g),$$

其中 $|G|$ 表示构成群 G 的置换个数，$\phi(g)$ 表示置换 g 的不动点个数，亦即满足 $g(a)=a$ 的元 $a\in S$ 个数．

证． 我们用两种不同的方式计算元偶 (g,a) 的个数 N，其中 $g\in G$，$a\in S$，且 $g(a)=a$．首先当 g 固定时，(g,a) 有 $\phi(g)$ 个，故 $N=\sum\limits_{g\in G}\phi(g)$．其次，对每个 $a\in S$，设有 $\eta(a)$ 个 $g\in G$ 以 a 为不动点，则有 $N=\sum\limits_{a\in S}\eta(a)$，故

$$\sum_{a\in S}\eta(a)=\sum_{g\in G}\phi(g). \tag{11}$$

为求 $\eta(a)$，我们将 G 中各置换 g 按其在元 a 上的取值 $g(a)$ 分类：

$$G=\bigcup_{i=1}^{r}G_i. \tag{12}$$

属于同一类 G_i 的两个置换 g_1，g_2 在 a 上取值相同：$g_1(a)=$



$g_2(a)$. 特别,令 G_1 由满足 $g(a)=a$ 的所有置换 g 组成. 由 $\eta(a)$ 的定义, $|G_1|=\eta(a)$. 今证

$$|G_i|=|G_1| \qquad (i=1,2,\cdots,r). \tag{13}$$

实际上,任意取定一元 $h\in G_i$, 则对每个 $f\in G_i$, 因 $h(a)=f(a)$, 故 $(fh^{-1})(a)=a$, 亦即任一 $f\in G_i$ 与 $g=fh^{-1}\in G_1$ 相对应,易见此为一一对应, 故有 (13) 式. 今进而证明, 若 $S(a)$ 为集合 S 中包含元 a 的等价类,则每个 G_i 与 $b\in S(a)$ 相对应. 事实上,属于同一 G_i 中的置换 f 与 g 在 a 上取值相同,令其共同值为 b: $f(a)=g(a)=b$, 并使 G_i 与 $b\in S(a)$ 相对应. 反之,任一 $b\in S(a)$, 由于 $b\sim a$, 故存在 $g\in G$ 使得 $b=g(a)$, 于是 b 对应于 g 所在的类 G_i. 易见此种对应为一一对应,故 G_i 的个数 r 等于 $|S(a)|$. 再由(12)及(13)式可见

$$\begin{aligned}|G| &= \sum_{i=1}^{r}|G_i| = \sum_{i=1}^{r}|G_1| \\ &= r\eta(a) = |S(a)|\eta(a),\end{aligned}$$

因此

$$\eta(a)=|G|/|S(a)|. \tag{14}$$

设集合 S 的等价类个数为 t: $S=\bigcup_{i=1}^{t}S_i$, 则由(11)式

$$\begin{aligned}\sum_{g\in G}\psi(g) &= \sum_{a\in S}|G|/|S(a)| \\ &= \sum_{i=1}^{t}\sum_{a\in S_i}|G|/|S(a)| \\ &= \sum_{i=1}^{t}|G| = t|G|.\end{aligned}$$

于是 $t=|G|^{-1}\sum_{g\in G}\psi(g)$, 引理证毕.



现在我们转而考察一般的染色问题．它是例 1 所提问题的直接推广．设给出有限集合 $S=\{a_1, a_2, \cdots, a_n\}$ 及其上的一个置换群 G，另有颜色集合 $C=\{c_1, c_2, \cdots, c_r\}$． 集合 S 的一种染色方式是指 S 到 C 中的一个映射 $f:f(a)=c$，$a\in S$，$c\in C$．这些映射的全体构成集合 C^S．显然 $|C^S|=|C|^{|S|}$．两种染色方式 f_1 与 f_2，若存在 $g\in G$，使得

$$f_1(ga)=f_2(a) \quad (\text{对所有的 } a\in S \text{ 成立}) \qquad (15)$$

（这里简记 $g(a)$ 为 ga），则称 f_1 与 f_2 等价，并记作 $f_1\sim f_2$．(15) 式也可写作 $f_1g=f_2$，它表示 f_2 等于先后两次映射 g 与 f_1 之积．容易证明上面引入的关系 $\sim$ 具有(10)中的三个性质，因而构成 C^S 中的一种等价关系． 于是 C^S 关于此种等价关系划分成诸等价类． 下面的 Pólya 基本定理给出了 C^S 中等价类的个数。

定理 A. C^S 中等价类个数等于

$$P_G(r, r, \cdots, r),$$

其中 $P_G(x_1, \cdots, x_n)$ 为群 G 的轮换指标，$r=|C|$．

我们将在下一节中给出这一定理的更一般形式及其证明。今列举该定理的若干应用例子．

例 5. 考察例 1 中所述无编号情形的解．此时 $S=\{a_1, \cdots, a_6\}$，群 G 如 (8) 所示，$C=\{A, B\}$，$n=6$，$r=2$．由 (9)式及定理 A 可见无编号情形的不等价染色方式种数为

$$P_G(2, 2, \cdots, 2)=(2^6+2^2\times 2^2+2\times 2^3)/4=24.$$

用尝试方法易列出这全部 24 种不等价的染色方式．

例 6. 考察图 3 所示的图 S，今用两种色 A 与 B 染 S 的四个顶点，问：若这四个顶点彼此没有区别，共有多少种不同的染色方式？ 这里若一种染色方式 f_1 经图形 S 的空间旋转后能与另一种染色方式 f_2 相重，则称 f_1 与 f_2 等价． 例如染色方式 $(a_1, a_2, a_3, a_4)=(A, A, B, B)$ 与 (A, B, B, A)



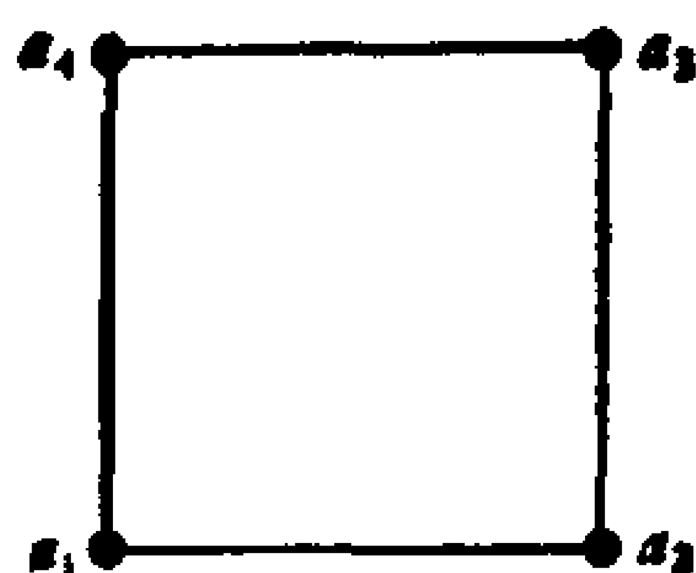


图 3.

等价，因将前者顺时针转动 90° 即得后者． 此时置换群G由下列诸置换组成：

$g_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234)$， 反时针转 90°；

$g_2 = (13)(24)$， 反时针转 180°；

$g_3 = (1423)$， 反时针转 270°；

$g_4 = (13)(2)(4)$， 绕轴 $\overline{a_2a_4}$ 转动 180°；

$g_5 = (24)(1)(3)$， 绕轴 $\overline{a_1a_3}$ 转动 180°；

$g_6 = (12)(34)$， 绕过 $\overline{a_1a_2}$ 及 $\overline{a_3a_4}$ 的两个中点之轴转 180°；

$g_7 = (14)(23)$， 仿上；

$e = (1)(2)(3)(4)$， 不动．

因此

$$P_G = (x_1^4 + 2x_1^2x_2 + 3x_2^2 + 2x_4)/8,$$

故不同的染色方式种数等于

$$P_G(2, 2, 2, 2) = (2^4 + 2 \times 2^3 + 3 \times 2^2 + 2 \times 2)/8 = 6.$$

易见这 6 种染色方式如下（见图 4）．

例 7（**环状字问题**）． r 个字母 $c_1, \cdots, c_r$ 可作成多少个长为 n 的环状字？（又见 3.1 节．）

此时 S 即为均匀排列在圆周上的 n 个点，在点 a_i 上放上字母 c_j 相当于将点 a_i 染以色 c_j，故 $C = (c_1, \cdots, c_r)$ 可



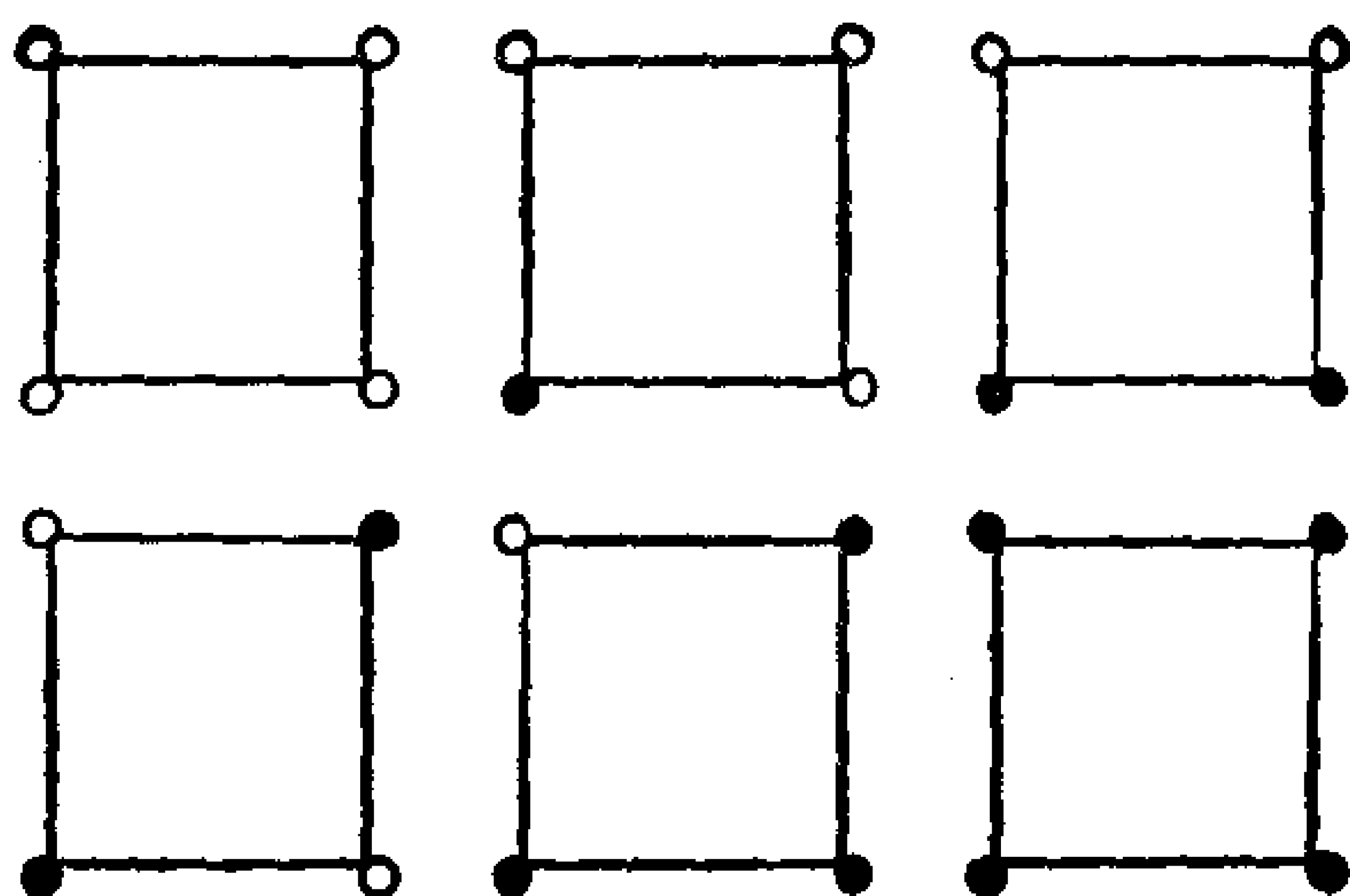


图 4.

视为色集合. 一个环状字 w_1 若经(平面)旋转能化至另一环状字 w_2, 则称字 w_1 与 w_2 等价. 问题即归为求出不等价的环状字个数.

此时置换群 G 由置换 $g=(123\cdots n)$ 及其各幂次 $g^2, g^3, \cdots, g^n=e$ 组成. 此种群称为**巡迴群**. 容易验证置换 g^d 可分解成 (d,n) 个长为 $n/(d,n)$ 的轮换之积,其中 (d,n) 表示 d 与 n 的最大公因子. 故群 G 的轮换指标为

$$P_G(x_1,\cdots,x_n)=\sum_{d=1}^{n}(x_{n/(d,n)})^{(d,n)}/n.$$

由 Euler 函数定义易知满足 $n/(d,n)=s$ 的 d 有 $\phi(s)$ 个(见 3.3 节),故上式可改写成

$$P_G(x_1,\cdots,x_n)=\sum_{s\mid n}\phi(s)(x_s)^{n/s}/n. \tag{16}$$

应用定理 A 可见环状字个数等于

$$N=(1/n)\sum_{d\mid n}\phi(d)r^{n/d}$$

$$=(1/n)\sum_{q\mid n}\phi(n/q)r^q. \tag{17}$$

但 $\phi(d)=\sum_{l\mid d}(\mu(l)/l)d$ (见(3.3)节),其中 μ 为 Möbius 函



数，故 $\phi(n/q)=\sum_{q|p|n}(n/p)\mu(p/q)$，代入(17)式得

$$N=\sum_{q|n}(1/n)\sum_{q|p|n}(n/p)\mu(p/q)r^q$$

$$=\sum_{p|n}(1/p)\sum_{q|p}\mu(p/q)r^q.$$

此与(3.1)节中用 Möbius 反演公式所得(3.1.10)式一致.

例 8 (**分放问题**). 将 4 个球 a, a, b, b 放入两个有编号的盒子 A, B 中,有几种放法?

此时 $S=\{a_1, a_2, a_3, a_4\}$, $a_1=a_2=a$, $a_3=a_4=b$. 因对任一种放法，对调 a_1 与 a_2 或 a_3 与 a_4 仍属同一种放法,故相应的置换群 G 为

$$g_1=(12)(3)(4),\quad g_2=(34)(1)(2),$$
$$g_3=(12)(34),\quad g_4=e,$$
$$P_G=(x_1^4+2x_1^2x_2+x_2^2)/4.$$

故不同的放法个数等于 $(2^4+2\times 2^3+2^2)/4=9$. 易见它们是

$$\varnothing|aabb,\ a|abb,\ b|aab,\ aa|bb,\ ab|ab,$$
$$aabb|\varnothing,\ abb|a,\ aab|b,\quad bb|aa.$$

5.2. Pólya-de Bruijn 计数定理

5.2.1. Pólya 计数定理的一般形式

如前,我们考察有限集合 S, C 及 S 上的置换群 G. 今设颜色集合 C 中的每一元 c, 赋有重量 $w(c)$ (它可以是实数或某个抽象域中的元), 又对于每个将 S 映入 C 的映射 $f\in C^S$, 定义其重量(乘积形式)为

$$w(f)=\prod_{a\in S}w(f(a)). \tag{1}$$



由此定义易证两个等价的映射 $f_1 \sim f_2$ 具有相同的重量：$w(f_1) = w(f_2)$. 实际上由 $f_1 \sim f_2$ 之定义知存在 $g \in G$ 使得 $f_2 = f_1 g$，故

$$w(f_2) = \prod_{a \in S} w(f_2(a)) = \prod_{a \in S} w(f_1(ga))$$

$$= \prod_{b \in S} w(f_1(b)) = w(f_1). \tag{2}$$

因此同属一个等价类 F 的函数便具同一重量，这一公共的重量值便可用来定义为等价类 F 的重量：

$$w(F) = w(f),\ f \in F. \tag{3}$$

今设集合 S 有一分划 $S = \bigcup_{i=1}^{k} S_i$，我们考察 C^S 中满足下列条件的函数 f 所构成的子集 R：每个 $f \in R$ 在各 S_i 上取常值，亦即当 $a, b \in S_i$ 时，$f(a) = f(b)$. 这种函数可看作复合函数 $f = \phi\psi$，其中函数 ψ 将 $a \in S_i$ 映成 i，而 ϕ 则将 $\{1, 2, \cdots, k\}$ 映入 C 中. 于是当分划 $S = \bigcup_{i} S_i$ 确定后，函数 ψ 是确定的，而 ϕ 则有 $|C|^k$ 种选择. 今证

命题 1. 设子集 $R \subset C^S$ 如上所述，则

$$\sum_{f \in R} w(f) = \prod_{i=1}^{k} \sum_{c \in C} (w(c))^{|S_i|}. \tag{4}$$

证. 设 $|S_i| = s_i$，则上式右边等于

$$(w(c_1)^{s_1} + \cdots + w(c_r)^{s_1})(w(c_1)^{s_2} + \cdots$$

$$+ w(c_r)^{s_2}) \cdots (w(c_1)^{s_k} + \cdots + w(c_r)^{s_k}), \tag{5}$$

其展开式的每一项 $w(c_{i_1})^{s_1} w(c_{i_2})^{s_2} \cdots w(c_{i_k})^{s_k}$ 相应于 ϕ 的一种选择：$\phi(1) = c_{i_1}$，$\phi(2) = c_{i_2}$，$\cdots$，故此展开项可以写成 $w(\phi(1))^{s_1} \cdots w(\phi(k))^{s_k}$. 而若 $f = \phi\psi$，则对 $a \in S_i$，$\psi(a) = i$，故



$$w(\phi(i))^{s_i} = \prod_{a \in S_i} w(\phi(\psi(a)))$$

$$= \prod_{a \in S_i} w(f(a)).$$

于是

$$\prod_{i=1}^{k} w(\phi(i))^{s_i} = \prod_{i=1}^{k} \prod_{a \in S_i} w(f(a))$$

$$= \prod_{a \in S} w(f(a)) = w(f).$$

因此(5)之展开式的每一项对应于一 $w(f)$,其中 $f = \phi\psi \in R$,反之亦然;且不同的展开项对应于不同的 f,故得(4)式.

今证当色集合 C 中诸元赋有重量时 Pólya 定理的一般形式.

定理 A. 设置换群 G 按上述方式将 C^S 划分成诸等价类 F,则

$$\sum_F w(F) = P_G\Big(\sum_c w(c),$$

$$\sum_c w(c)^2,\ \sum_c w(c)^3,\ \cdots\Big)$$

其中 $\sum\limits_c$ 表示对所有的 $c \in C$ 求和,P_G 为群 G 的轮换指标.特别当 C 中诸元 $w(c) = 1$ 时,此时 $w(F) = 1$,即得等价类 F 的个数为 $P_G(|C|, |C|, \cdots)$,即上节之定理 A.

证. 设 w 为函数 $f \in C^S$ 所能取到的重量之一.考察

$$R_w = \{f | f \in C^S,\ w(f) = w\}.$$

对于任一 $g \in G$,由(2)式知 $w(f) = w(fg^{-1})$,故 $f \in R_w \Rightarrow fg^{-1} \in R_w$. 因此每个 $g \in G$ 引出映 R_w 到自身的一个映射:$g \to \pi_g$,

$$\pi_g f = fg^{-1},$$



由此，便可在 R_w 中引入等价关系：对 $f_1, f_2 \in R_w$，若存在 $g \in G$，使得 $f_2 = \pi_g f_1$，或即 $f_2 = f_1 g^{-1}$，则称 f_2 与 f_1 等价．由 Burside 引理，R_w 中的等价类个数等于

$$|G|^{-1} \sum_{g \in G} \psi_w(g), \tag{6}$$

其中 $\psi_w(g)$ 表示 R_w 中满足 $\pi_g f = f$ 亦即 $f = fg$ 的函数 f 个数．由定义可见 R_w 中的每个等价类的重量都等于 w，因此若将(6)式乘以 w，然后对所有可能的 w 求和，便得 C^S 中全部等价类的重量之和，即

$$\sum_F w(F) = |G|^{-1} \sum_w \sum_{g \in G} \psi_w(g) w.$$

因显然

$$\sum_w \psi_w(g) w = \sum_{\{f|f=fg\}} w(f),$$

故

$$\sum_F w(F) = |G|^{-1} \sum_{g \in G} \sum_{\{f|f=fg\}} w(f). \tag{7}$$

为计算 $\sum_{\{f|f=fg\}} w(f)$，设 g 属于类型 $\{b_1, b_2, b_3, \cdots\}$，即

$$g = \underbrace{(a)(b)\cdots(d)}_{b_1} \underbrace{(eh)\cdots\quad\cdots}_{b_2} \cdots(rs\cdots q).$$

取 $S_1 = \{a\}, S_2 = \{b\}, \cdots, S_{b_1+1} = \{e, h\}, \cdots, S_{\Sigma b_i} = \{r, s, \cdots, q\}$．于是当 $f = fg$ 时，因 $f(a) = f(ga) = f(g^2 a) = \cdots$，所以 f 在每个 S_i 上取常值，应用(4)式即得

$$\sum_{\{f|f=fg\}} w(f) = (\sum w(c))^{b_1} (\sum w(c)^2)^{b_2} \cdots,$$

代入(7)式即证得本定理．

例 1．　考察上节例 1 之染色问题．如果我们不仅要知道有多少种不等价的染色方法，且需更细致地知道，有多少种不等价的染色方法使得图 S 中有 k 个点染以色 A，则可赋予



色 A 以重量 x，色 B 以重量 1：$w(A)=x$, $w(B)=1$. 这样使得 S 中有 k 个点染以色 A 的每一种染色方式 F 均有重量 $w(F)=x^k$. 于是若以 α_k 记满足 $w(F)=x^k$ 的诸不等价染色方式个数，则 $\sum\alpha_k x^k=\sum w(F)$. 注意到此例 $P_G=(x_1^6+x_1^2x_2^2+2x_2^3)$，故

$$\sum_F w(F)=((1+x)^6+(1+x)^2(1+x^2)^2$$
$$+2(1+x^2)^3)/4$$
$$=x^6+2x^5+6x^4+6x^3+6x^2+2x+1.$$

例如其中的一项 $6x^4$ 表明，4 个点染以色 A 的不等价染色方式共有 6 种. 易验这 6 种是

$$(a_1a_2\cdots a_6)=AAAABB,\ AAABAB,\ AAABBA,$$
$$AABBAA,\ ABABAA,\ ABBAAA.$$

(参见图 5.1.1.)

例 2 (**环状字问题**). 在上节中我们已证得(见 (5.1.16) 式)：r 个字母 $c_1, c_2, \cdots, c_r$ 共可作成

$$N=(1/n)\sum_{d|n}\phi(d)r^{n/d}$$

个不同的环状字. 如果我们需要更细致地知道这 N 个环状字中，字母 c_1 恰用了 n_1 次，c_2 用了 n_2 次，$\cdots$，c_r 用了 n_r 次的环状字个数为多少，这里 $n_1, n_2, \cdots, n_r$ 为 n 的一个特定的分划：$n=n_1+\cdots+n_r$，为此，我们可赋予不同的字母以不同的重量：$w(c_i)=\alpha_i$，此时对应于上述问题的等价类便具有重量 $\alpha_1^{n_1}\alpha_2^{n_2}\cdots\alpha_r^{n_r}$. 故由定理 A 及 (5.1.15) 式可见，所求环状字个数 $N(n_1, n_2, \cdots, n_r)$ 等于下列多项式中 $\alpha_1^{n_1}\alpha_2^{n_2}\cdots\alpha_r^{n_r}$ 前的系数：

$$P_G(\sum\alpha_i, \sum\alpha_i^2, \sum\alpha_i^3, \cdots)$$
$$=\frac{1}{n}\sum_{d|n}\phi(d)(\alpha_1^d+\alpha_2^d+\cdots+\alpha_r^d)^{n/d},$$



亦即

$$N(n_1, n_2, \cdots, n_r) = \frac{1}{n} \sum_{d|(n_1,\cdots,n_r)} \phi(d) \binom{n/d}{n_1/d, n_2/d, \cdots, n_r/d}.$$

这里 $(n_1, n_2, \cdots, n_r)$ 表示 $n_1, n_2, \cdots, n_r$ 的最大公因子 g，和式遍及 g 的所有因子 d(包括 1 和 g 自身).

这一结果最早是在傅钟孙 [11] 中得到的. 但在该文中上式系经直接推理得出,并未应用 Pólya 计数定理,故证明较长些.

可注意的是，上面所讨论的环状字实质上是平面的环状字,亦即两个环状字若经(平面上的)旋转可以彼此重合,则视为同一个字，傅钟孙教授在上述文中还进而仔细地讨论了空间环状字的个数. 此时，环状字仍视为均匀分布在一个圆环上的 n 个字母,两个环状字若能经空间的运动(即除去绕圆心 O 的旋转外,还有以某个直径为轴的反射)相互重合，则视为同一字. 假设圆环上的 n 个字母按顺时针方向顺次为 $a_1, a_2, \cdots, a_n$，则反射方式计有两种:

(i) 绕轴 Oa_i 转动 180°, 此种反射记作 V_i;

(ii) 绕轴 Ob_i 转动 180°,此处 b_i 为弧 $\overset{\frown}{a_i a_{i+1}}$ 的中点，此种反射记作 W_i.

又以 R_k 泛指某一种反射,即 V_i 或 W_i.

对于旋转，则引入记号 O_n^d 表示绕圆心 O 顺时针转动 $2\pi d/n$ 个弧度. 同样以 O_i 泛指某个旋转. 不难证明

(i) 连续两次反射等于一次旋转，即 $R_1R_2 = O_3$ (例如 $V_{i+1}V_1 = O_n^{2i}$ 等，此处 $V_{i+1}V_1$ 表示先后两次反射之积: 先经反射 V_1, 后经反射 V_{i+1});

(ii) 每个反射 R 都可以表示成反射 W_n 与旋转之积,例如 $W_i = O_n^{-i} W_n O_n^i$ 等;



(iii) $R_iO_jR_i = O_j^{-1}$，例如 $V_iO_n^kV_i = O_n^{-k}$.

此处 O_j^{-1} 表示旋转 O_j 之逆，例如 $(O_n^k)^{-1} = O_n^{-k} = O_n^{n-k}$.（注意对反射而言，其逆为自身：$R_j^{-1} = R_j$.）

由上述三点可见，与此计数问题相应的置换群 G 乃由 $g = (123\cdots n)$（它与旋转 O_n^1 相应）及 $h = (1, n)(2, n-1)(3, n-2)\cdots$（它与反射 W_n 相应）生成. 换言之，G 为包含 g 与 h 的最小置换群. 此种群称为**二面体群**，一般记作 D_n. 它的轮换指标将在下一节中给出. 利用该轮换指标便可求出空间环状字的个数. 但群 D_n 的轮换指标的讨论在 5.3 节中未予写出，故下面我们根据傅钟孙 [11] 一文给出的更为初等一些的推理方式，将计数结果另行说明于下.

上面我们已经看到，用 n_1 个字母 $c_1, \cdots, n_r$ 个字母 c_r 共可作出

$$N = \frac{1}{n}\sum_{d|(n_1,\cdots,n_r)} \phi(d)\binom{n/d}{n_1/d, \cdots, n_r/d}$$

个旋转不等价的环状字 $A_1, \cdots, A_N$. 将这些环状字全体所成集合记作 $\mathscr{A}$：

$$\mathscr{A} = \{A_1, A_2, \cdots, A_N\}.$$

在这 N 个环状字中，尽管不可能由其中一个经某种旋转 O_j 化至另一个，但却可能经某个反射 R_k 化至另一个. 今证这种因反射引出的转化只能成对地出现，也就是说：在集合 $\mathscr{A}$ 中不可能存在三个不同的环状字 A_i, A_j 与 A_k，使得 (i) $R_1(A_i) \sim A_j$, $R_2(A_j) \sim A_k$；或者 (ii) $R_1(A_i) \sim A_j$, $R_2(A_i) \sim A_k$. 这里 $\sim$ 表示旋转等价，$R_i(A)$ 表示字 A 经反射 R_i 后所得者. 实际上，在情形 (i) 将有 $A_j = O_1R_1(A_i)$, $A_k = O_2R_2(A_j)$，从而 $A_k = O_2R_2O_1R_1A_i = O_2R_2R_1(R_1O_1R_1)A_i = O_2R_2R_1O_1^{-1}$. 但如前所述 $R_1R_2 = O_3$，故 $A_k = O_2O_3O_1^{-1}(A_i)$，此即 $A_k \sim A_i$，此不可能，因 $\mathscr{A}$ 中诸字 A_i 彼此不旋转等



价。对于情形 (ii)，注意到 $R(A_i)=A_j\Rightarrow R(A_j)=A_i$，故同情形 (i)，也不可能。

由此可见，集合 $\mathscr{A}$ 中的字可分成二类：一类是对称的，亦即此种环状字经反射后与自身相(旋转)等价：$R(A)\sim A$；另一类是非对称的，此种字总是成对地出现：(A_{i_1}, A_{i_2})，(A_{i_3}, A_{i_4})，$\cdots$. 同一对中的两个字可经反射相互转化，而不同对的字则不存在此种转化。今设 $\mathscr{A}$ 中对称的字有 s 个，则不对称的元便有 $N-s$ 个，且由上面所作的分析容易明白：由 n_1 个字母 c_1，$\cdots$，n_r 个字母 c_r 构成的不同环状字个数等于

$$s+\frac{1}{2}(N-s)=\frac{1}{2}(N+s)$$

个。下面我们来定出对称的环状字个数 $s=s(n_1,\cdots,n_r)$. 首先我们注意到一个对称的环状字 A 易证为完全对称的，亦即存在一个反射 R 使得 $RA=A$. 此时，除去对称轴的一端或二端处出现的那种字母其个数可能为奇数外，其余的字母其个数因完全对称性必为偶数，因此对于一个对称字 A，n_1，$\cdots$，n_r 中至多出现二个奇数，此即

$$s(n_1,\cdots,n_r)=0$$

(当 $n_1, n_2, \cdots, n_r$ 中奇数个数 $\geqslant 3$ 时)。

当 $n_1,\cdots,n_r$ 中奇数个数 $\leqslant 2$ 时，与奇数 $n_i=2k_i+1$ 相应的字母 c_i 必定有一个出现在对称轴的一端且仅只一端，剩下 $2k_i$ 个字母 c_i 在对称轴的两侧各有 $k_i=\left[\frac{n_i}{2}\right]$ 个。对于与偶数 $n_j=2k_j$ 相应的字母 c_j，显然在对称轴的两侧各有 $k_j=\left[\frac{n_j}{2}\right]$ 个. 因此在对称轴的一侧计有 $\left[\frac{n_i}{2}\right]$ 个字母 $c_i(i=1, 2, \cdots, r)$，计有



$$\begin{pmatrix} \left[\frac{n_1}{2}\right]+\left[\frac{n_2}{2}\right]+\cdots+\left[\frac{n_r}{2}\right] \\ \left[\frac{n_1}{2}\right], \left[\frac{n_2}{2}\right], \cdots, \left[\frac{n_r}{2}\right] \end{pmatrix}$$

种不同的排列方式，故见

$$s(n_1, \cdots, n_r) = \begin{pmatrix} \left[\frac{n_1}{2}\right]+\left[\frac{n_2}{2}\right]+\cdots+\left[\frac{n_r}{2}\right] \\ \left[\frac{n_1}{2}\right], \left[\frac{n_2}{2}\right], \cdots, \left[\frac{n_r}{2}\right] \end{pmatrix}$$

（当 $n_1, \cdots, n_r$ 中奇数个数 $\leqslant 2$ 时）．

由上述诸式便可推出下面的

定理（傅钟孙［11］）．由 n_1 个字母 c_1，n_2 个字母 c_2，$\cdots$，n_r 个字母 c_r 构成的不同的(空间)环状字个数为

$$\frac{1}{2}\left(\sum_{d|(n_1,\cdots,n_r)} \phi(d) \begin{pmatrix} n/d \\ n_1/d, n_2/d, \cdots, n_r/d \end{pmatrix} + s(n_1, \cdots, n_r)\right),$$

其中 $\phi(d)$ 为 Euler 函数，$(n_1, \cdots, n_r)$ 表示 $n_1, \cdots, n_r$ 的最大公约数 g，和式遍及 g 的所有因子 d（包括 1 与 g 自身），又

$$s(n_1, \cdots, n_r) = \begin{cases} 0, & \text{若 } n_1, \cdots, n_r \text{ 中奇数个数} \geqslant 3; \\ \begin{pmatrix} \left[\frac{n_1}{2}\right]+\cdots+\left[\frac{n_r}{2}\right] \\ \left[\frac{n_1}{2}\right], \cdots, \left[\frac{n_r}{2}\right] \end{pmatrix}, & \text{其他情形}. \end{cases}$$

5.2.2. 基本计数定理的推广

定理 A 指出了当集合 S 上给出置换群 G 时不等价的染色



方式个数，在许多应用问题中，我们还须考察集合 C 上也给出置换群 H 的情形。例如在分放问题中，当球和盒子均为无编号时便属这种情形。de Bruijn[42] 首先考察了这一情形。下面我们将引述相应的结果并举例加以说明，详细的证明可见 Beckenbach [30]。

设在元集合 S 上给出置换群 G，色集合 C 上给出置换群 H。此时两种染色方式 $f_1, f_2 \in C^S$，若存在 $g \in G, h \in H$ 使得 $f_2 = hf_1g$，亦即

$$f_2(a) = hf_1(ga), \quad a \in S, \tag{8}$$

则称 f_1 与 f_2 等价并记作 $f_1 \sim f_2$。容易证明这是一种等价关系，在此种等价关系下，C^S 划分为诸等价类，其个数由下面的 de Bruijn 定理给出：

定理 B. 设 S, C, G, H 如上所述，则 C^S 中等价类个数为

$$P_G\left(\frac{\partial}{\partial z_1}, \frac{\partial}{\partial z_2}, \frac{\partial}{\partial z_3}, \cdots\right) P_H(e^{z_1+z_2+z_3+\cdots}, e^{2(z_2+z_4+z_6+\cdots)}, e^{3(z_3+z_6+z_9+\cdots)}, \cdots) \tag{9}$$

在 $z_1 = z_2 = z_3 = \cdots = 0$ 处的值。

这一公式虽然形式相当优美，但因涉及到很多微分运算，应用起来有时并不很方便。在 Harary and Palmer [78] 中，将此公式改写成下面的形式，在一些场合运用更见方便些。

定理 B′. 设 S, C, G, H 如前所述，则 C^S 中的等价类个数为

$$|H|^{-1} \sum_{h \in H} P_G(c_1(h), c_2(h), \cdots, c_n(h)), \tag{10}$$

其中

$$c_k(h) = \sum_{s|k} s b_s(h),$$

而 $(b_1(h), b_2(h), \cdots)$ 为 h 所属的类型。



例 2（分放问题）．考察 5.1 节的例子中所述的问题，但设盒子 A，B 没有区别．此时置换群 H 即为群 S_2． 故 $P_H=(x_1^2+x_2)/2$，P_G 则如前为 $(x_1^4+2x_1^2x_2+x_2^2)/4$，故不同的放法个数为

$$\frac{1}{4}\left(\left(\frac{\partial}{\partial z_1}\right)^4+2\left(\frac{\partial}{\partial z_1}\right)^2\left(\frac{\partial}{\partial z_2}\right)\right.$$

$$\left.+\left(\frac{\partial}{\partial z_2}\right)^2\right)\left(\frac{1}{2}((e^{x_1+x_1})^2+e^{2x_2})\right)_{x=0}$$

$$=(2^4+2\times 2^3+2^3)/8=5.$$

易验这 5 种分放方式为

$\{aabb\}$，$\{\varnothing\}$；$\{a\}$，$\{abb\}$；$\{b\}$，$\{aab\}$；

$\{aa\}$，$\{bb\}$；　$\{ab\}$，$\{ab\}$．

由于分放问题在应用中经常遇到，今再举一例说明定理 B 在四种不同类型的分放问题中的应用．

例 3．　将 4 个球放入 3 个盒子中有几种放法？

情形 (i)．球和盒子均有编号． 此时 G 与 H 均只含一个恒等置换．$P_G=x_1^4$，$P_H=x_1^3$，故分放方式个数等于

$$(\partial/\partial z_1)^4(e^{x_1})^3_{x=0}=3^4=81.$$

此时分放方式个数等于 3 个字母的可重复的 4-排列个数．

情形 (ii)．球有编号，而盒子没有编号． 此时 $P_G=x_1^4$，$P_H=P_{S_3}=(x_1^3+3x_1x_2+2x_3)/6$．此时，对类型为 $\{3,0,0\}$ 的 $h\in H$ 有 $c_1(h)=b_1(h)=3$；对类型为 $\{1,1,0\}$ 的 h，$c_1(h)=b_1(h)=1$；对类型为 $\{0,0,2\}$ 的 $h\in H$，有 $c_1(h)=b_1(h)=0$，故由定理 B′，不同的放法个数为

$$(3^4+3\times 1^4+2\times 0^4)/6=14.$$

此时分放方式个数，由第二类 Stirling 数的定义(2.4 节)，易见应等于 $S(4,1)+S(4,2)+S(4,3)=1+7+6=14$．

情形 (iii)．球无编号，盒子有编号． 此时 $P_G=P_{S_4}=$



$(x_1^4 + 6x_1^2x_2 + 8x_1x_3 + 3x_2^2 + 6x_4)/24$, $P_H = x_1^3$, $e = (1)(2)(3)$ 为H中唯一的置换,故 $c_k(h) = b_1(h) = 3$, 由定理 B′ 可见放法个数为

$$P_G(3, 3, \cdots) = (3^4 + 6 \times 3^3 + 8 \times 3^2 + 3 \times 3^2 + 6 \times 3)/24 = 15.$$

情形 (iv). 球和盒子均无编号. 此时 P_G 如上, $P_H = P_{S_3}$, 应用定理 B′ 易计得放法个数为

$$\begin{aligned}&(P_G(3, 3, 3, 3) + 3P_G(1, 3, 1, 3) \\ &\quad + 2P_G(0, 0, 3, 0))/6 \\ &= (15 + 3 \times 3 + 2 \times 0)/6 = 4.\end{aligned}$$

易验这 4 种放法为 $\{aaaa\}, \{\varnothing\}, \{\varnothing\}$; $\{aaa\}, \{a\}, \{\varnothing\}$; $\{aa\}, \{aa\}, \{\varnothing\}$; $\{a\}, \{a\}, \{aa\}$. 在这种情形分放方式个数等于 $P(4, 1) + P(4, 2) + P(4, 3) = 1 + 2 + 1 = 4$, 其中 $P(n, m)$ 表示将正整数 n 分划成 m 个正整数之和(诸加项次序不计)的不同方式个数.

Pólya 计数定理的另一种推广方式是计算在单个颜色置换下不变的等价类个数. 假设给出元集合 S, 其上置换群 G 及色集合 C 如前. 同样, 群 G 将 C^S 划分成诸等价类 F. 今若给出色集合 C 上的一个置换 h, 一个等价类 F 若满足 $hF \subset F$, 亦即 $f \in F \Rightarrow hf \in F$, 则称此等价类 F 关于色置换 h 不变或称在置换 h 下不变.

定理 C (de Bruijn). 关于置换 h 不变的等价类之重量和

$$\sum_{F, hF \subset F} w(F) = P_G(p_1, p_2, \cdots, p_n),$$

其中 $P_G(x_1, \cdots, x_n)$ 为群 G 的轮换指标, 而

$$p_k = \sum_{\{c \mid h^k c = c, c \in C\}} w(c) w(hc) \cdots w(h^{k-1}c).$$

(当 $\{c \mid h^k c = c\} = \varnothing$ 时, 令 $p_k = 0$.) 尤当所有的 $w(c) =$



1 时,即得关于 h 不变的等价类个数为 $P_G(l_1, l_2, \cdots, l_n)$, 其中 l_k 为置换 h^k 的不动点个数.

定理A是定理C当 $h = e$ (恒等置换)时的特例.

例 4. 考察5.1节中的例8. 我们来计算关于 $h = (A, B)$ 为不变的等价类,亦即将盒子 A 与 B 对换后不变的放法个数. 此时 $hc = c$ 无解, 而 $h^2 = e$, 故 $l_2 = 2$, 因此所求个数等于

$$P_G(0, 2) = ((x_1^4 + 2x_1^2x_2 + x_2^2)/4)_{x_1=0, x_2=2} = 2^2/4 = 1.$$

易见这唯一的等价类为 $bc|bc$.

例 5. 考察5.1节中的例4. 仍令 $h = (A, B)$, 求对换染色 A, B 后不变的染色方式个数. 此时, $P_G = (x_1^6 + x_1^2x_2^2 + 2x_2^3)/4$, 而 h 同上例, 故所求个数等于

$$P_G(0, 2) = 2 \times 2^3/4 = 4.$$

易验这4种染色方式为

$$(a_1, a_2, \cdots, a_6) = AABBAB, ABABAB, ABBAAB, ABBABA.$$

Pólya 方法近年来得到了种种推广,如见 de Bruijn [45], Parthasarathy and Sridharan [124], Williamson [159] 等.

5.3. 置换群轮换指标的计算

本节讨论几种应用中最常遇见的置换群的轮换指标的计算方法,并给出由两个置换群衍生出来的群如 $A \times B$, A^B 等轮换指标的计算式,本节中 P_G 均记作 $P(G)$.

1. $G = \{e\} = I_n$. 亦即 G 仅由一个恒等置换 e 组成. 此时显然

$$P(I_n) = x_1^n. \tag{1}$$



2. $G=S_n$(n 个文字的对称群). 对此有

$$P(S_n;x_1,\cdots,x_n)=\sum\frac{1}{b_1!b_2!\cdots b_n!}\times\left(\frac{x_1}{1}\right)^{b_1}\left(\frac{x_2}{2}\right)^{b_2}\cdots\left(\frac{x_n}{n}\right)^{b_n}. \tag{2}$$

式中和式遍及不定方程 $b_1+2b_2+\cdots+nb_n=n$ 的所有非负解 $\{b_1,b_2,\cdots,b_n\}$. 此式乃下面的命题的直接推论.

命题 1. S_n 中类型为 $\{b_1,b_2,b_3,\cdots\}$ 的置换个数 $h(b_1,b_2,\cdots)$ 等于

$$((b_1!1^{b_1})(b_2!2^{b_2})\cdots(b_n!2^{b_n}))^{-1}n!.$$

证. 每个类型为 $\{b_1,b_2,\cdots\}$ 的置换 g 形如

$$\underbrace{(a)(b)\cdots(h)}_{b_1}\ \underbrace{(rs)\cdots(uv)}_{b_2}\cdots\cdots\cdots\underbrace{(pq\cdots l)}, \tag{3}$$

去掉括号即得 n 个文字的一个排列 $(ab\cdots hrs\cdots l)$. 但在(3)中, b_i 个长为 i 的轮换因子间次序是随意的,故有 $b_i!$ 种书写方式;而每个长为 i 的轮换因子又有 i 种书写方式: $(jk\cdots t)=(k\cdots tj)=(\cdots tjk)=\cdots$, 由此可见每一个置换(3)对应于 $(b_1!1^{b_1})(b_2!2^{b_2})\cdots(b_n!n^{b_n})$ 个不同的排列,且不同的置换对应不同的排列,故

$$n!=h(b_1,b_2,\cdots)(b_1!1^{b_1})(b_2!2^{b_2})\cdots(b_n!n^{b_n}).$$

由此便推出(3)式.

比较(2)与(2.3.17)式可见, $P(S_n)$ 还可用 Bell 多项式表出:

$$\begin{aligned}P(S_n;x_1,\cdots,x_n)\\&=(1/n!)Y_n(x_1,1!x_2,2!x_3,\cdots,\\&\quad(n-1)!x_n).\end{aligned} \tag{4}$$

由(2)式用归纳法并可推出 $P(S_n)$ 的递推式如下:

$$P(S_n)=1/n\sum_{k=1}^{n}x_kP(S_{n-k}). \tag{5}$$



3. **交代群 A_n.** 它由 S_n 中所有偶置换(即所属类型 $\{b_1, b_2, \cdots\}$ 满足 $b_2+b_4+b_6+\cdots=$ 偶数的置换)组成。此时由命题 1 可知

$$P(A_n; x_1, \cdots, x_n)=\sum\frac{1+(-1)^{b_2+b_4+b_6+\cdots}}{b_1!b_2!\cdots b_n!}\times\left(\frac{x_1}{1}\right)^{b_1}\left(\frac{x_2}{2}\right)^{b_2}\cdots\left(\frac{x_n}{n}\right)^{b_n}, \tag{6}$$

和式遍及范围同(2)式。(6)式还可写成

$$P(A_n; x_1, \cdots, x_n)=P(S_n; x_1, \cdots, x_n)+P(S_n; x_1, -x_2, x_3, -x_4, \cdots). \tag{7}$$

4. **巡迴群 C_n.** 它由 $g=(123\cdots)$ 的各个幂次组成.它的轮换指标已在 5.1 节中得出为

$$P(C_n)=(1/n)\sum_{k|n}\phi(k)x_k^{n/k}, \tag{8}$$

其中 $\phi(k)$ 为 Euler 函数。

5. **二面体群 D_n.** 它由 $g=(123\cdots n)$ 及 $h=(1,n)\times(2,n-1)(3,n-2)\cdots$生成,亦即为包含 g 与 h 的最小置换群,由 $2n$ 个置换组成。我们已在 5.2.1 节的例 2 中遇见过。它的轮换指标为

$$P(D_n)=(1/2)P(C_n)+\begin{cases}(1/2)x_1x_2^{(n-1)/2}, & n\text{ 为奇数},\\ (1/4)(x_2^{n/2}+x_1^2x_2^{(n-2)/2}), & n\text{ 为偶数}.\end{cases} \tag{9}$$

此群与著名的"染色项链"问题有关。所谓"染色项链"即为用不同颜色的珠子串成的圈,实际上即为由 r 个字母构成的一个(空间的)环状字(5.2.1 节)。

在应用中,我们还需考察由已知群引出的群。

1. **群之(简单积)** GH. 设 G 为 X 上的置换群,H 为 Y 上的置换群。假设 X 与 Y 无公共元,则可定义 $X\cup Y$ 上的群 GH 如下:



$$GH = \{(g, h) \mid g \in G, h \in H\},$$

$$(g, h)(a) = \begin{cases} g(a), & \text{对 } a \in X; \\ h(a), & \text{对 } a \in Y. \end{cases} \tag{10}$$

由此定义易证

$$P(GH; x_1, x_2, \cdots, x_{n+m}) = P(G; x_1, \cdots, x_n) P(H; x_1, \cdots, x_m). \tag{11}$$

这里 $|X| = n$, $|Y| = m$, 于是 $|X \cup Y| = |X| + |Y| = m + n$.

例如

$$P(S_2S_3) = P(S_2)P(S_3) = (1/2)(x_1^2 + x_2)(1/6)(x_1^3 + 3x_1x_2 + 2x_3)$$
$$= (1/12)(x_1^5 + 4x_1^3x_2 + 3x_1x_2^2 + 2x_1^2x_3 + 2x_2x_3).$$

2. 群之直积 $G \times H$. 设 G, H 各为集合 X 与 Y 上的置换群,定义集合 $X \times Y$ 上的群 $G \times H$ 如下:

$$G \times H = \{(g, h) \mid g \in G, h \in H\},$$

$$(g, h)(x, y) = (gx, hy), (x, y) \in X \times Y. \tag{12}$$

易证所有形如(12)的置换确实构成 $X \times Y$ 上的置换群.

命题 2. 设 $|X| = n$, $|Y| = m$.

$$P(G \times H; x_1, x_2, \cdots, x_{mn}) = (|G||H|)^{-1} \sum_{\substack{g \in G \\ h \in H}} \prod_{k, l \geq 1} x_{[k,l]}^{(k,l) b_k c_l}. \tag{13}$$

其中 $[k, l]$ 与 (k, l) 各表示 k 与 l 的最小公倍数及最大公约数, 而 $\{b_1, b_2, \cdots\}$ 及 $\{c_1, c_2, \cdots\}$ 各为置换 g 与 h 所属的类型.

证. 设 $x \in X$ 出现在置换 g 的一个长为 k 的轮换因子中, $y \in Y$ 出现在置换 h 的一个长为 l 的轮换因子中, 于是 $g^k x = x$, $h^l y = y$. 由定义 $(g, h)^p(x, y) = (g^p x, h^p y)$, 故



易见，满足 $(g, h)^p(x, y) = (x, y)$ 的最小正整数 $p = [k, l]$. 于是 kl 个元偶 $A = \{(u, v) | u = g^i(x), v = h^j(y); i = 1, \cdots, k, j = 1, \cdots, l\}$ 被划分成 $kl/[k, l] = (k, l)$ 个组，每一组对应于置换 (g, h) 的一个长为 $[k, l]$ 的轮换因子. 实际上，在 $A \in X \times Y$ 中引入等价关系：$(u, v) \sim (u', v')$ 当且仅当 $(u', v') = (g, h)(u, v)$，即易证明各等价类中元数相同，每个等价类对应于 (g, h) 的一个轮换因子，便可证得上述断言. 于是 g 的每一个长为 k 的轮换因子连同 h 的每个长为 l 的轮换因子，对应于 (g, h) 的 kl 个长为 $[k, l]$ 的轮换因子. 由此可见 (g, h) 有 $b_k c_l (k, l)$ 个长为 $[k, l]$ 的轮换因子. (13)式得证.

与此定理相对应，我们引入多项式的直积如下：

$$x_i^a \times x_j^b = x_{[i,j]}^{(i,j)ab},$$

$$f \times (g + h) = f \times g + f \times h,$$

$$(gh) \times f = f \times (gh) = (f \times g)(f \times h). \tag{14}$$

其中 f 与 g 均为 $x_1, x_2, \cdots$ 的多项式，例如

$$x_1^2 \times x_3 = x_3^2,$$

$$x_2 \times (x_1 x_2) = (x_2 \times x_1)(x_2 \times x_2) = (x_2)(x_2^2) = x_2^3.$$

引进这种运算后，(13)式便可写成更易记忆的形式：

$$P(G \times H) = P(G) \times P(H). \tag{15}$$

例 1. 记 $S_2^n = S_2 \times S_2 \times \cdots \times S_2 = \times_{i=1}^n S_2$，则

$$P(S_2^n) = (x_1^{2^n} + (2^n - 1) x_2^{2^{n-1}})/2^n. \tag{16}$$

此式易由 $P(S_2) = (x_1^2 + x_2)/2$, $P(S_2^{k+1}) = P(S_2^k) \times P(S_2)$ 及(14)式归纳证明之.

3. **幂次群** H^G. 设 G, H 如上述，定义 Y^X 上的群 H^G 如下：

$$H^G = \{(g, h) | g \in G, h \in H\},$$

$$(g, h) f(x) = h f(gx), \quad f \in Y^X, x \in X. \tag{17}$$



易证上式所确定的 H^G 确为一群。

命题 3. （见 Harary and Palmer [78].） 设 $|X|=n$, $|Y|=m$, 则

$$P(H^G; x_1, x_2, \cdots, x_{m^n})$$
$$=(|G||H|)^{-1}\sum_{\substack{g\in G\\ h\in H}}\prod_k x_k^{b_k(g,h)}.$$

其中

$$b_1(g,h)=\prod_{k\geq 1}\sum_{r|k}(rc_r)^{b_k},$$

$$b_k(g,h)=\left(\frac{1}{k}\right)\sum_{r|k}\mu(r,k)b_1(g^r,h^r) \quad (k>1). \quad (18)$$

$(b_1, b_2, \cdots)$ 与 $(c_1, c_2, \cdots)$ 各为置换 g 与 h 所属的类型, $\mu(r,k)$ 为经典的 Möbius 函数.

还可以引出其他形式的由已知群衍生得来的群，下面仅讨论下一节中用到的两种.

设 X 为一有限集合,以 $X^{(2)}$ 表示 X 的 2-子集, 亦即形如 $\{a,b\}$ $(a, b\in X, a\neq b)$ 的无序元偶的全体. 每个 X 上的置换 g, 引出 $X^{(2)}$ 上的置换 $\bar{g}$ 如下:

$$\bar{g}\{a,b\}=\{g(a), g(b)\}. \quad (19)$$

于是每个 X 上的置换群 G 便引出 $X^{(2)}$ 上的置换群 $G^{(2)}=\{\bar{g}|g\in G\}$, 称为 G 的**偶群**. 例如取 $X=\{1,2,3\}$, $G=S_3=\{e, g_1, g_2, g_3, g_4, g_5\}$, 此时 $X^{(2)}=\{a,b,c\}$, 其中

$$a=\{1,2\}, \quad b=\{1,3\}, \quad c=\{2,3\},$$
$$e=(1)(2)(3), \quad g_1=(1)(23), \quad g_2=(2)(13),$$
$$g_3=(3)(12), \quad g_4=(123), \quad g_5=(132).$$

于是 $\bar{g}_1(a)=\bar{g}_1\{1,2\}=\{g_1(1), g_1(2)\}=\{1,3\}=b$, 同样 $\bar{g}_1(b)=\{1,2\}=a$, $\bar{g}_1(c)=c$, 此即 $\bar{g}_1=(c)(a,b)$. 同样方式可得 $\bar{g}_2=(b)(a,c)$, $\bar{g}_3=(a)(b,c)$, $\bar{g}_4=(acb)$,



$\bar{g}_5 = (abc)$ 及 $\bar{e} = (a)(b)(c)$，此即

$$P(S_3^{(2)}; x_1, x_2, x_3) = (x_1^3 + 3x_1x_2 + 2x_3)/6.$$

在一般情形，有

命题 4.

$$P(S_n^{(2)}; x_1, x_2, \cdots, x_N) = \sum((b_1!1^{b_1})(b_2!2^{b_2})\cdots)^{-1}f_b(x). \qquad (20)$$

其中 $N = \binom{n}{2}$，$b = (b_1, b_2, \cdots)$，$x = (x_1, \cdots, x_N)$，和式遍及范围同(2)式，而

$$f_b(x) = \prod_k x_{2k+1}^{kb_{2k+1}} \prod_k (x_k x_{2k}^{k-1})^{b_{2k}} x_k^{k\binom{b_k}{2}} \prod_{r<t} x_{[r,t]}^{(r,t)b_rb_t}. \qquad (21)$$

其证的基本思想是对于确定的 g:$\bar{g}\{a, b\} = \{g(a), g(b)\}$，区分两类不同的元偶 $\{a, b\}$：在第一类中，a，b 同属 g 的一个轮换因子，这种元偶共有 $\sum_k \binom{b_k}{2}$ 个，此时当 k 为奇数时，g 的每个长为 k 的轮换因子便引出 $\bar{g}$ 的 $(k-1)/2$ 个长为 k 的轮换因子，此即(21)式中第一个乘积项的由来．相仿，第二个乘积项的头一个因子由 g 的偶数长轮换因子引出；在第二类中，a，b 属于不同的轮换因子，由此引出(21)中后两项乘积．

由(21)式可见．$P(S_n^{(2)})$ 可按下列步骤得出：

(i) 写出 $f = P(S_n)$.

(ii) 对 f 中的每个单项式 $x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}$ 经步骤(iii)转换为 $x_1^{c_1}x_2^{c_2}\cdots x_N^{c_N}$，$N = \binom{n}{2}$，单项式前系数不变，即得出 $P(S_n^{(2)})$.

(iii) 转换方式：

(a) 当 k 为奇数时，$x_k^{b_k} \to x_k^{b_k(kb_k-1)/2}$;



(b) 当 k 为偶数时，$x_k^{b_k} \to (x_{k/2} x_k^{(kb_k-2)/2})^{b_k}$;

(c) 作出 $x_1^{b_1} \times x_2^{b_2} \times \cdots \times x_n^{b_n} = \prod_{i<j} x_{[i,j]}^{(i,j)b_ib_j}$.

将所得三类项相乘即得 $x_1^{c_1} x_2^{c_2} \cdots$.

例如为求 $P(S_4^{(2)})$，首先写出

$$P(S_4) = (x_1^4 + 6x_1^2 x_2 + 8x_1 x_3 + 3x_2^2 + 6x_4)/24.$$

对于第一项 x_1^4，显然 $x_1^4 \to x_1^{(4/2)(4-1)} = x_1^6$；对于第二项 $x_1^2 x_2$，

$$x_1^2 \to x_1^{(2-1)2/2} = x_1, \quad x_2 \to (x_1 x_2^0)^1 = x_1,$$

$$x_1^2 \times x_2 = x_{[2,1]}^{(2,1)2} = x_2^2.$$

故 $x_1^2 x_2$ 应转换成 $x_1 x_1 x_2^2 = x_1^2 x_2^2$. 同样方式 $x_1 x_3 \to x_3^2$ 等，即得

$$P(S_4^{(2)}) = (x_1^6 + 6x_1^2 x_2^2 + 8x_3^2 + 3x_1^2 x_2^2 + 6x_2 x_4)/24. \quad (22)$$

最后我们讨论群 $\boldsymbol{S_n \otimes G}$，它定义为

$$S_n \otimes G = \{(\beta, \sigma) | \beta \in G^n, \sigma \in S_n\}.$$

其中 G 为 X 上的一个置换群，$G^n = G \times G \times \cdots \times G$，$\beta = (g_1, \cdots, g_n) \in G^n$，$g_i \in G$. (β, σ) 作为 $X^n = X \times X \times \cdots \times X$ 上的一个置换定义为

$$(\beta, \sigma)(x_1, \cdots, x_n) = (g_1 x_{\sigma^{-1}(1)}, \cdots, g_n x_{\sigma^{-1}(n)}). \quad (23)$$

由此定义易见，若记 $\sigma(\beta) = (g_{\sigma^{-1}(1)}, \cdots, g_{\sigma^{-1}(n)}) \in G^n$，则

$$(\beta_2, \sigma_2)(\beta_1, \sigma_1) = (\beta_2 \sigma_2(\beta_1), \sigma_2 \sigma_1).$$

命题 5.

$$P(S_n \otimes I_2) = \sum((b_1! 1^{b_1})(b_2! 2^{b_2}) \cdots)^{-1}$$

$$\mathop{\times}_{i=1}^{n} \left(\prod_{d|i} x_d^{g_i(d)}\right)^{\times b_i}. \quad (24)$$

其中和式遍及范围同(2)式，而

$$g_i(s) = \begin{cases} (1/s) \sum\limits_{d|s} 2^d \mu(s/d), & 若 s|i; \\ 0, & 若 s\nmid i. \end{cases}$$



$\mu(k)$ 为经典的 Möbius 函数. 又

$$f^{\times i}=f\times f\times\cdots\times f\ (i\ 项).$$

命题 6.

$$P(S_n\otimes S_2)=\sum((b_1!2^{b_1})(b_2!4^{b_2})(b_3!6^{b_3})\cdots)^{-1}$$

$$\mathop{\times}_{i=1}^{n}\left(\prod_{d|i}x_d^{g_i(d)}+\prod_{\substack{d|2i\\ d\nmid i}}x_d^{h_i(d)}\right)^{\times b_i}. \tag{25}$$

其中和式遍及范围及 $g_i(d)$ 同命题 5, 而

$$h_i(2s)=(1/2s)\sum_{\substack{d|2s\\ d\nmid s}}2^{d/2}\mu(2s/d). \tag{26}$$

命题 5 与 6 之证明见 Harrison and High [80], 在该文中并给出了 $P(S_n\otimes G)$ 的一般公式.

5.4. Pólya 计数方法的应用

在 5.1 与 5.2 节中,结合理论的陈述已列举了若干应用例子,本节再给出两类应用例子.

5.4.1. 无编号图的计数

我们在 5.1 节中已经列出了无编号图和有编号图两种不同的概念. 下面我们给出无编号图的严格定义.

考察具有相同顶点集合 V 的两个图 $X_1=(V,E_1)$ 和 $X_2=(V,E_2)$, E_1 与 E_2 分别为图 X_1 与 X_2 的边集合. 有如上节所述, 顶点集合 V 上的每个置换 g, 引出边集合 E_i 上的置换 $\bar{g}$:$\bar{g}\{a,b\}=\{g(a),g(b)\}$, 其中 $a,b\in V$, $\{a,b\}$ 为图 X 中的边. 下面我们将限于考察无向图, 此时元偶 $\{a,b\}$ 便为无序元偶,从而 E_1, E_2 均为 $V^{(2)}$ 的一个子集合. 对于两个这样的图 X_1 与 X_2, 若存在顶点集合的一个置换 g,



使得 $\bar{g}E_1 = E_2$, 亦即 $E_2 = \{g(a), g(b)\}|\{a, b\} \in E_1\}$, 则称两个图 X_1 与 X_2 同构. 图 1 表出了两个同构的图.

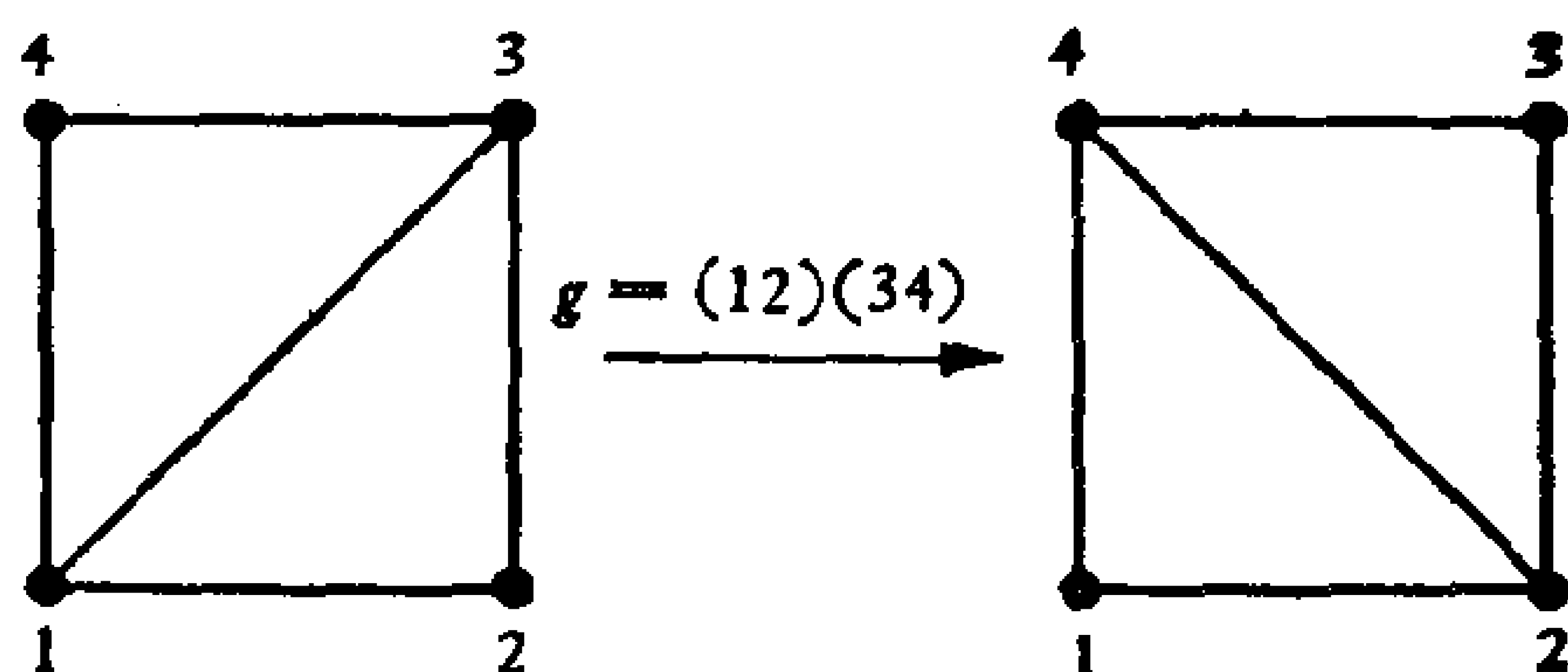


图 1. 两个同构的图

显然,同构关系是一种等价关系,它将具 n 个顶点的所有图的集合划分成诸等价类, 每个等价类便称作一个 "无编号图". 例如 4 个顶点的无编号图共有 11 个,它们是

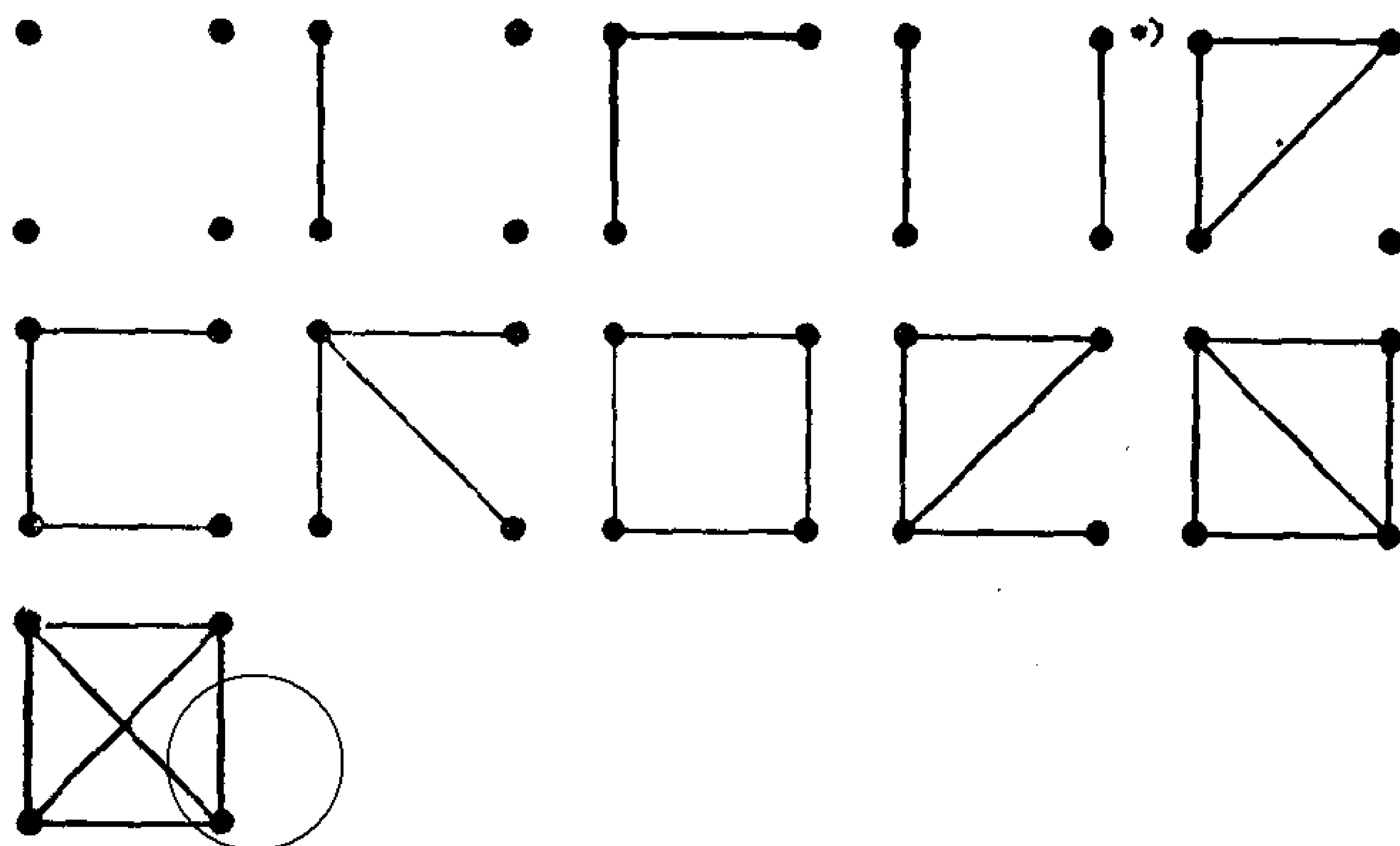


图 2. 4 个顶点的无编号图,其中*)为自补图

定理 A. n 个顶点的无编号图个数为 $P(S_n^{(2)}; 2, 2, \cdots)$. 更细地说,具有 n 个顶点, k 条边的无编号图个数等于 $P(S_n^{(2)}; 1 + x, 1 + x^2, 1 + x^3, \cdots)$ 的展开式中 x^k 前的系数.



例如,由 $P(S_4^{(2)})$ 的表示式(5.3.22),

$$
\begin{aligned}
P(S_4^{(2)}, 1+x, 1+x^2, \cdots) &= ((1+x)^6 + 6(1+x)^2(1+x^2)^2 \\
&\quad + 8(1+x^3)^2 + 3(1+x)^2(1+x^2)^2 \\
&\quad + 6(1+x^2)(1+x^4))/24 \\
&= 1 + x + 2x^2 + 3x^3 + 2x^4 + x^5 + x^6,
\end{aligned}
$$

故共有 $1+1+2+3+2+1+1=11$ 个无编号图. 又由其中的一项如 $3x^3$ 知其中有 3 条边的图有 3 个等等.

定理 A 的证明. 考察 V 的所有 2-子集 $V^{(2)}$, $|V^{(2)}| = n(n-1)/2$, 其中 $n=|V|$. $V^{(2)}$ 即由所有可能的 $n(n-1)/2$ 条边组成. 今用两种色 A, B 将 $V^{(2)}$ 中各边任意染色, 每一种染色方式即对应于一个图 (V, E), 其中 E 由 $V^{(2)}$ 中色为 A 的边组成. 由图的同构定义可见,两个图 (V, E_1) 与 (V, E_2) 同构当且仅当相应的两种染色方式 f_1 与 f_2 等价, 亦即存在 $V^{(2)}$ 的一个置换 $g \in S_n^{(2)}$, 使得 $f_2\{a, b\} = f_1 g_1\{a, b\}$. 应用 Pólya 基本计数定理 5.2. A 即得证本定理.

在上面证明中,我们看到 $V^{(2)}$ 的每一种染色方式引出两个图 $X=(V, E)$ 与 $\overline{X}=(V, \overline{E})$, 其中 E 由色为 A 的边组成, $\overline{E}$ 由色为 B 的边组成. 图 $\overline{X}$ 称作是图 X 的补图. 换言之,若抹去图 X 中的所有边,而将原来不相邻的各对点都用边相连, 便得 $\overline{X}$. 一个图 X 若与其补图 $\overline{X}$ 同构, 则称 X 为自补图. 由上述证明可知,每个自补图对应于 $V^{(2)}$ 的一种关于色置换 (A, B) 为不变的染色方式的等价类,故由定理 5.2.C 即得

定理 B. 具有 n 个顶点的(无编号)自补图的个数等于

$$P(S_n^{(2)}; 0, 2, 0, 2, \cdots).$$

例如 $n=4$ 时,其个数等于 $((6x_2x_4)/24)_{x_2=x_4=2}=1$. 这唯一的自补图见图 2 所示.



关于 Pólya 方法在图的各种计数问题中的应用，详见 Harary and Palmer [79]. 图的计数问题在诸如化学，遗传学等一类涉及分子结构图形的学科中均有遇见. Pólya 本人即应用他所创立的这一计数方法计算了一类碳氢分子结构的个数. 见 Pólya [127], Balaban and Harary [27], Read [131] 及 Gordon [71] 等.

5.4.2. Boole 函数的分类

布尔 (Boole) 函数在现代计算机、继电器等逻辑线路的设计中有重要的应用. 一个 n 个变量的布尔函数 $f(x_1, \cdots, x_n)$ 乃集合 Z_2^n 到 Z_2 中的一个映射，其中 $Z_2 = \{0, 1\}$, $Z_2^n = Z_2 \times Z_2 \times \cdots \times Z_2 = \{(x_1, x_2, \cdots, x_n) | x_i \in Z_2\}$. 因此 n 个变量的布尔函数共有 $|Z_2^{(Z_2^n)}| = 2^{2^n}$ 个. 布尔量 0 与 1 共有三种基本运算：加法、乘法与取补，分别定义为 $1 + x = 1$, $0 + x = x$ (加法); $1 \cdot x = x$, $0 \cdot x = 0$ (乘法)及 $\bar{0} = 1$, $\bar{1} = 0$ (取补). 我们将讨论三种最简单的等价关系：(i) 变量取补；例如对 $f(x_1, x_2, x_3) = x_1 + x_2\bar{x}_3$, 则认为 $f(x_1, \bar{x}_2, \bar{x}_3) = x_1 + \bar{x}_2 x_3$ 等与 $f(x_1, x_2, x_3)$ 等价；(ii) 变量下标的置换，例如认为 $f(x_2, x_3, x_1) = x_2 + x_3\bar{x}_1$ 等与 $f(x_1, x_2, x_3)$ 等价；(iii) 上述两种变换的复合，如 $f(\bar{x}_2, x_3, \bar{x}_1) = \bar{x}_2 + x_3 x_1$ 等认为与 $f(x_1, x_2, x_3)$ 等价.

对于第一种等价关系，即变量取补，相应的置换群为 C_2^n:

$$C_2^n = \{i = (i_1, i_2, \cdots, i_n) | i_k = 0 \text{ 或 } 1\}.$$

变元 $x = (x_1, \cdots, x_n) \in Z_2^n$ 经过置换 i 后得 $i(x_1, \cdots, x_n) = (x_1^{i_1}, \cdots, x_n^{i_n})$, 其中 $x_k^0 = x_k$, $x_k^1 = \bar{x}_k$. 易见 C_2 与 S_2 同构，从而 C_2^n 与 S_2^n 同构，于是 $P(C_2^n) = P(S_2^n)$. 应用 Pólya 定理并(5.3.16)可见下面的定理成立.

定理 C. n 个变量的布尔函数全体关于群 C_2^n 的等价类



个数等于

$$P(C_2^n;\ 2,\ 2,\ \cdots) = (2^{2^n} + (2^n - 1)2^{2^{n-1}})/2^n.$$

例如当 $n = 2$ 时，个数等于 $(2^4 + (2^2 - 1)2^2)/4 = 7$。不难列出这 7 种等价类为

$\{0\}$,

$\{x_1x_2,\ x_1\bar{x}_2,\ \bar{x}_1x_2,\ \bar{x}_1\bar{x}_2\}$,

$\{x_1,\ \bar{x}_1\}$, $\{x_2,\ \bar{x}_2\}$,

$\{x_1 \oplus x_2,\ x_1 \equiv x_2\}$,

$\{x_1 + x_2,\ \bar{x}_1 + x_2,\ x_1 + \bar{x}_2,\ \bar{x}_1 + \bar{x}_2\}$,

$\{1\}$.

其中 $x_1 \oplus x_2 = x_1\bar{x}_2 + \bar{x}_1x_2$, $(x_1 \equiv x_2) = x_1x_2 + \bar{x}_1\bar{x}_2$.

由 Pólya 定理及命题 5.3.5 可见

定理 D. n 个变量的布尔函数全体关于变量下标置换群 $S_n \otimes I_2$ 的等价类个数为

$$\begin{aligned} P(S_n \otimes I;\ 2,\ 2,\ \cdots) &= \sum((b_1!1^{b_1})(b_2!2^{b_2})\cdots)^{-1} \\ &\quad \mathop{\times}_{i=1}^{n} \left(\prod_{d|i} 2^{g_i(d)}\right)^{\times b_i}. \end{aligned}$$

例如 $n = 2$ 时，易计得 $P(S_2 \otimes I_2) = (x_1^4 + x_1^2x_2)/2$，故有 $(2^4 + 2^3)/2 = 12$ 个等价类．易验它们是

$\{0\}$,

$\{x_1x_2\}$, $\{\bar{x}_1\bar{x}_2\}$, $\{x_1\bar{x}_2,\ \bar{x}_1x_2\}$,

$\{x_1,\ x_2\}$, $\{x_1 \oplus x_2\}$, $\{x_1 \equiv x_2\}$, $\{\bar{x}_1,\ \bar{x}_2\}$,

$\{\bar{x}_1 + \bar{x}_2\}$, $\{x_1 + x_2\}$, $\{x_1 + \bar{x}_2,\ \bar{x}_1 + x_2\}$,

$\{1\}$.

最后讨论布尔函数在下标置换及变量取补变换下等价类的个数．此时相应群易见为 $S_n \otimes C_2$．故有

定理 E. n 个变量的布尔函数全体关于下标置换及变



量取补的等价类个数为

$$P(S_n \otimes C_2;\ 2,\ 2,\ \cdots).$$

例如 $n=2$ 时，易计得 $P(S_2 \otimes C_2) = (x_1^4 + 3x_2^2 + 2x_1^2x_2 + 2x_4)/8$，故等价类个数为 $(2^4 + 3 \times 2^2 + 2 \times 2^3 + 2 \times 2)/8 = 6$．易验这 6 个等价类为

$\{0\}$,

$\{x_1x_2,\ x_1\bar{x}_2,\ \bar{x}_1x_2,\ \bar{x}_1\bar{x}_2\}$,

$\{x_1,\ x_2,\ \bar{x}_1,\ \bar{x}_2\}$, $\{x_1 \oplus x_2,\ x_1 \equiv x_2\}$,

$\{x_1 + x_2,\ x_1 + \bar{x}_2,\ \bar{x}_1 + x_2,\ \bar{x}_1 + \bar{x}_2\}$,

$\{1\}$.

一个布尔函数的重量定义为其真值表中 1 的个数．在上面 $n=2$ 的三种情形下等价类表中，我们将重量相同的等价类排在同一行，从上到下按重量为序列出．运用赋有重量形式的 Pólya 计数定理，可以计算出三种情形下重量为 k 的等价类个数．读者可作为练习试算之．

在 Harrison [81] 中还讨论了在更广的变量代换 (即变量的可逆线性或仿射变换)下的等价类个数．

5.5. 纠错编码理论中的码字重量分布问题

设 X, Y 为两个有限集合，G 与 H 分别为 X 与 Y 上的置换群，如前，记 Y^X 为映 X 到 Y 中的映射全体．Pólya-de Braijn 定理虽然很好地解决了 Y^X 关于群 G 与 H 的等价类个数的计算问题，但在应用中仍有其局限性：(i) 它给出的是整个集合 Y^X 的等价类个数，而在某些应用中，我们要求对 Y^X 的某个子集 $R \subset Y^X$ 计算其等价类个数；(ii) 它只给出了等价类的个数，而未告诉我们每个等价类中有多少个元；(iii) 对于 Y^X 的每个等价类，未给出 $f \in F$ 的特征．当然这三个问



题的一般性解决是相当困难的，有待于群论方法的进一步发展和完善．本节我们将以纠错编码理论中的码字重量分布问题为例，说明群论方法在上述三种场合下的应用．

所谓纠错编码是指将一组信息 $a=(a_1, a_2, \cdots, a_k)$ 按一定法则转换成码字 $C=(c_1, c_2, \cdots, c_n)$，使得在 C 的传送过程中所出现的少量差错能被接收者所发现并加以纠正．这种将信息字 a 转换成码字的过程即称作编码．最简单的编码方式是在 a 的最后一位后面添加一个奇偶校核位，这样传送时每一重错将改变 $\sum_i c_i$ 的奇偶性，便可为接收者所发觉．但这种编码并不能纠正所发生的差错，对二重错也无法查知．现代的纠错编码理论则提供了种种纠错能力强得多的编码方式，Reed-Muller（RM）码即为一例．一般（$a_1, \cdots, a_k$）及（$c_1, \cdots, c_n$）中诸分量 a_i，c_j 均等于0或1，此时称 C 中 $c_i=1$ 的个数为码字的重量，对于一个特定的码字集合 C，求出其中码字重量等于 k 的码字个数称为码字的重量分布问题，它与码的纠错能力之分析有密切关系（见 Berlekamp [37]）．迄今完整地求得重量分布的码类并不多．下面我们将限于讨论 RM 码．在5.5.1节中我们将应用 Dickson 有关正交群的经典结果导出二阶 RM 码的重量分布；在5.5.2节中则给出了三阶 RM 码的重量分布的部分解．

5.5.1. 二阶 *RM* 码的重量分布

r 阶 RM 码的定义在3.3节中已有述及，二阶 RM 码 R 即为 $GF(2)$ 上形如

$$f(x_1, \cdots, x_m)=\sum_{\substack{i,j=1 \\ i<j}}^{n} a_{ij}x_ix_j$$



$$+\sum_{k=1}^{m} b_k x_k + b. \tag{1}$$

的二次多项式的全体,其中系数 $a_{ij}, b_k \in GF(2)$. 此种多项式有 $\binom{m}{0}+\binom{m}{1}+\binom{m}{2}=k$ 个系数,每个系数可取 0 或 1,故共有 2^k 个码字,它的编码方式是将长为 k 的信息字 $(a_1, \cdots, a_k)$ 看作 $(a_{12}, a_{13}, \cdots, b_1, \cdots, b_m, b_0)$,作出多项式(1),便得码字 $C=(c_1, \cdots, c_n)=(f(0), f(1), \cdots, f(n))$,其中 $n=2^m-1$,而当 i 的二进展开为 $i=\sum_{k=0}^{m-1} i_k 2^k$ 时,定义 $f(i)=f(i_{m-1}, i_{m-2}, \cdots, i_1, i_0)$. 例如当 $m=4$ 时,$k=11$,信息字 $(1100\cdots0)$ 对应于多项式 $f(x_1, \cdots, x_m)=x_1x_2+x_1x_3$. 此时 $f(0)=f(0,0,0,0)=0$, $f(1)=f(0,0,0,1)=0, \cdots, f(12)=f(1,1,0,0)=1$ 等,因此相应的码字 $c=(0,0,\cdots,1,0,0)$. 若定义 $|f|_m$ 为 $f(0), f(1), \cdots, f(n)$ 中 1 的个数,则此例 $|x_1x_2+x_1x_3|_m=2^{m-2}=4$. 二阶 RM 码的重量分布问题即为对 $k=0, 1, \cdots, 2^m$,求出 $|f|_m=k$ 的形如(1)的多项式 f 的个数.

定义 1. 设 $y=(y_1, \cdots, y_m)$, $x=(x_1, \cdots, x_m)$,若变换 $T: y=Tx$ 由下式确定

$$y_i=\sum_{j=1}^{m} \alpha_{ij} y_j+\alpha_{i0} \quad (i=1, \cdots, m), \tag{2}$$

其中系数 $\alpha_{ij} \in GF(2)$,与 x, y 无关,且 $\det(\alpha_{ij}) \neq 0$,则称 T 为可逆仿射变换,简称 A 变换;而当 $\alpha_{i0}=0\ (i=1, \cdots, m)$ 时,称 T 为可逆齐次线性变换,简称 L 变换. A 变换的全体构成 $GF(2)^m$ 上的置换群,记作 A_m. L 变换的全体相应记作 L_m.

一个 A 变换 T 既然作为 $GF(2)^m$ 上的一个置换,当 x 遍



及 $GF(2)^m$ 时，$y = Tx$ 亦然，故由 $|f|_m$ 的定义可见：$|f|_m$ 在变元的 A 变换下不变，亦即若 $g(y) = g(Tx) = f(x)$，则 $|g|_m = |f|_m$. 例如 T: $y_1 = x_1$, $y_2 = x_2 + x_3$，将 $x_1x_2 + x_1x_3$ 变至 y_1y_2，于是 $|x_1x_2 + x_1x_4|_m = |y_1y_2|_m$. 基于多项式重量的这一性质，我们分三步来解码字集合 R 的重量分布问题：(i) 应用置换群 L_n 将 R 划分成等价类，于是每个等价类中多项式的重量相等；(ii) 求出每个等价类中 $f(x)$ 的一般形式（即所谓典式），并进一步求出该等价类中多项式的个数；(iii) 将重量等于 k 的所有等价类中元数相加，便得出满足 $|f|_m = k$ 的多项式 f 个数.

在这一问题中，我们所要划分的不是 m 个变量的多项式全体，而只是它的一个子集 R；我们还需求出每个等价类中元的个数及其特征，这便是我们在本节开始时所提及的三个方面. 为了完成 (i), (ii) 两步，我们引用 Dickson [56] 中的两个经典结果：

定理 A. 设 $f \in R$，若 f 的二次项系数不全为零，则总可经变元的 L 变换化至下面的几种典式之一：

$$y_1y_2 + y_3y_4 + \cdots + y_{2r-1}y_{2r} + \alpha, \tag{3}$$

$$y_1y_2 + y_3y_4 + \cdots + y_{2r-1}y_{2r} + y_{2r-1} + y_{2r} + \beta, \tag{4}$$

$$y_1y_2 + y_3y_4 + \cdots + y_{2r-1}y_{2r} + y_{2r+1} + \gamma. \tag{5}$$

其中 $\alpha, \beta, \gamma = 0$ 或 1，$r \geqslant 1$.

今记

$$\Phi_{1r} = y_1y_2 + y_3y_4 + \cdots + y_{2r-1}y_{2r}, \tag{6}$$

$$\Phi_{2r} = y_1y_2 + y_3y_4 + \cdots + y_{2r-1}y_{2r} + y_{2r-1} + y_{2r} + 1. \tag{7}$$

定义 2. 一个多项式 $f(x)$ 若满足

$$f(x) = f(Tx), \tag{8}$$

则称 $f(x)$ 在变换 T 下不变. (8)式也可写作 $Tf = f$.



如前所述，使得 f 不变的 $T\in L_m$ 之全体构成一个群，记作 $G(f)$，其阶 $|G(f)|$ 记作 $J(f)$.

定理 B. 使得 Φ_{kr} 不变的 L 变换 $z_i=\sum_{j=1}^{r}\alpha_{ij}y_j$ $(i=1,2,\cdots,r)$ 的个数等于

$$N(\Phi_{1r})=2(2^r-1)(4^{r-1}-1)4^{r-1}\cdots(4-1)4, \quad (9)$$

$$N(\Phi_{2r})=2(2^r+1)(4^{r-1}-1)4^{r-1}\cdots(4-1)4. \quad (10)$$

今证

命题 1. s 个相互独立的线性式

$$y_i=\sum_{j=1}^{m}\alpha_{ij}x_j+\alpha_{i0} \qquad (i=1,\cdots,s)$$

共有

$$2^s(2^m-1)(2^m-2)\cdots(2^m-2^{s-1})$$
$$=2^{s(s+1)/2}(2^m-1)(2^{m-1}-1)\cdots(2^{m-s+1}-1)$$

组，而当要求 $\alpha_{i0}=0$ $(i=1,2,\cdots,s)$ 时共有 $(2^m-1)\cdot(2^m-2)\cdots(2^m-2^{s-1})$ 组.

实际上，选择 $y_1=\sum_j\alpha_{1j}x_j+\alpha_{10}$ 时，α_{10} 可任意选取，$\alpha_{11},\cdots,\alpha_{1m}$ 只需不全为零，故共有 $2(2^m-1)$ 种取法. 一般当 $y_1,\cdots,y_k$ 取定后，选择 y_{k+1} 时，$\alpha_{k+1,0}$ 随意，而 $(\alpha_{k+1,1},\cdots,\alpha_{k+1,m})$ 的选择只需不是 $\sum_{i=1}^{k}\beta_i(\alpha_{i1},\cdots,\alpha_{im})$ 即可，故共有 $2(2^m-2^k)$ 种取法.

推论. (i) $|A_m|=2^m(2^m-1)(2^m-2)\cdots(2^m-2^{m-1})$; (11)

(ii) $|L_m|=(2^m-1)(2^m-2)\cdots(2^m-2^{m-1})$; (12)

(iii) 使得 $\Phi_{tr}(t=1,2)$ 不变的 L 变换 $T\in L_m$ 的个数，亦即 $J(\Phi_{tr})$ 为



$$J(\Phi_{tr}) = N(\Phi_{tr})(2^m - 2^r)\cdots(2^m - 2^{m-1})$$
$$(t = 1, 2). \tag{13}$$

(13)式可从 $N(\Phi_{tr})$ 的定义及命题 (1) 直接推出，式中因子 $(2^m - 2^r)\cdots(2^m - 2^{m-1})$ 相应于变换 T 中 $z_{r+1}, \cdots, z_m$ 的不同取法.

命题 2. R 中与 Φ_{tr} 关于置换群 L_m 为等价的多项式个数等于

$$|S(\Phi_{tr})| = (2^m - 1)(2^m - 2)\cdots(2^m - 2^{2r-1})/N(\Phi_{tr})$$
$$(t = 1, 2). \tag{14}$$

此式可从(5.1.14)及(12),(13)推出. 至此，我们便可给出二阶 RM 码重量分布问题的完全解.

定理 C. (i) 在二阶 RM 码 R 中，非零码字多项式 $f(x_1, \cdots, x_m)$ 的重量必取

$$2^{m-1} + \varepsilon 2^{m-1-r} \qquad (\varepsilon = 0, 1 \text{ 或} -1,\ 0 < r \leqslant [m/2])$$

形式.

(ii) 重量为 $2^{m-1} + 2^{m-1-r}$ 的码字个数等于

$$N_r = \frac{2^{r^2+r}(2^m - 1)(2^{m-1} - 1)\cdots(2^{m-2r+1} - 1)}{(4^r - 1)(4^{r-1} - 1)\cdots(4 - 1)}, \tag{15}$$

重量为 $2^{m-1} - 2^{m-1-r}$ 的码字个数同上 $(N_0 = 1)$.

(iii) 重量为 2^{m-1} 的码字个数等于

$$N = 2\left(2^{m(m+1)/2} - \sum_{r=0}^{[m/2]} N_r\right). \tag{16}$$

证. 因当 $g = f + 1$ 时，$|g|_m = 2^m - |f|_m$，故重量为 $2^{m-1} + w$ 的码字个数与重量为 $2^{m-1} - w$ 的码字个数相等. 又 $|f|_m = 0$ 当且仅当 $f = 0$，故我们可以只限于讨论满足 $0 < |f|_m \leqslant 2^{m-1}$ 的码字多项式.

若 $f \in R$ 的二次项系数不全为零，则由定理 A，f 必可经 L 变换化至(3),(4),(5)三种典式之一. 但易计得 $|\Phi_{1r}|_m =$



$|\Phi_{2r}|_m = 2^{m-1} - 2^{m-1-r}$. 又(5)式所示 f 之重量为 2^{m-1}. 故有结论 (i); 此外可见: 若 $|f|_m = 2^{m-1} - 2^{m-1-r}$, 则 f 必可化至 Φ_{1r} 或 Φ_{2r} 形式. 再由(9),(10)及(14)式可见重量为 $2^{m-1} - 2^{m-1-r}$ 的多项式个数等于

$$
\begin{aligned}
&(2^m - 1)(2^m - 2)\cdots(2^m - 2^{2r-1}) \\
&\quad \times (N(\Phi_{1r})^{-1} + N(\Phi_{2r})^{-1}). \\
&= \frac{(2^m - 1)(2^m - 2)\cdots(2^m - 2^{r-1})}{2(4^{r-1} - 1)4^{r-1}\cdots(4 - 1)4} \\
&\quad \times \left(\frac{1}{2^r - 1} + \frac{1}{2^r + 1}\right) \\
&= (15)\text{式的右边}.
\end{aligned}
$$

当 $f \in R$ 不含二次项时, f 必可经 L 变换化至 0, 1, 或 $y_1 + \alpha$ 三种形式之一, 但 $|y_1 + \alpha|_m$ 显然等于 2^{m-1}, 故在 $0 < |f|_m \leqslant 2^{m-1}$ 时, 剩下的情形必为 $|f|_m = 2^{m-1}$. 既然 R 中全部码字的个数等于 $2^{\binom{m}{2}+\binom{m}{1}+1} = 2^{(m(m+1)/2)+1}$,即见(16)式成立.

定理 C 系 Sloane and Berlekamp 在[144]中首先得出,但推证较长. 此处证明利用了 Dickson 的一个经典结果,故推证比较简短. 这一证明的思想是 McEliece 所指出的[1)].

5.5.2. 三阶 *RM* 码中一类码字的计数

尽管现有的文献对各种域上二次形的分类已有相当丰富的论述,但对三次形的分类迄今的结果极少,因此当我们运用上节中的方法于三阶 RM 码的重量分布问题时,只能得出部分的结果.

下面我们用 R_3 表示 $GF(2)$ 上三次多项式 $f(x_1, \cdots,$

1) 因 McEliece 的工作未能查到,本节证明系作者据这一思想推演得来.



$x_m) = \sum \alpha_{ijk}x_ix_jx_k + \alpha$ 的全体. 在 Kasami and Tokura [94] 中证得

定理 D. 若 $f \in R_3, 0 < |f|_m < 2^{m-2}$, 则经变元的 A 变换可将 f 化至下列典式之一:

$$\Phi_1 = y_1y_2y_3 + y_4y_5y_6,$$

$$\Phi_{2r} = y_1(y_2y_3 + y_4y_5 + \cdots + y_{2r}y_{2r+1}).$$

其重量 $|\Phi_1|_m = 2^{m-2} - 2^{m-5}$, $|\Phi_{2r}| = 2^{m-2} - 2^{m-2-r}$.

由此定理便可进而推出三阶 RM 码中满足 $0 < |f|_m < 2^{m-2}$ 的各类码字的个数. 为叙述简单见, 假定 $m \geqslant 7$, 此时便有

定理 E. 以 $N_{m,k}$ 记三阶 RM 码中重量为 k 的码字个数, $m \geqslant 7$, 则当

$$0 < |f|_m < 2^{m-2} \tag{17}$$

时, $|f|_m$ 必取 $w(r) = 2^{m-2} - 2^{m-2-r}$ 形式, 其中 $1 \leqslant r \leqslant [(m-1)/2]$, 且

$$N_{m,w(1)} = 2^3 \frac{(2^m-1)(2^{m-1}-1)(2^{m-2}-1)}{(2^3-1)(2^2-1)(2-1)},$$

$$N_{m,w(3)} = 2^{14} \frac{(2^m-1)(2^{m-1}-1)\cdots(2^{m-5}-1)}{(2^3-1)^2(2^2-1)^2(2-1)^2} + 2^{13} \frac{(2^m-1)(2^{m-1}-1)\cdots(2^{m-6}-1)}{(4^3-1)(4^2-1)(4-1)},$$

$$N_{m,w(r)} = 2^{r^2+r+1} \frac{(2^m-1)(2^{m-1}-1)\cdots(2^{m-2r}-1)}{(4^r-1)(4^{r-1}-1)\cdots(4-1)} \quad (r = 2 \text{ 或 } r \geqslant 4). \tag{18}$$

对于 $|f|_m = 2^{m-2}$ 的码字, 则有屠规彰[15], [16].

定理 F. 若 $f \in R_3, |f|_m = 2^{m-2}$, 则 f 可经变元的 A 变换化至下列典式之一:

$$\Psi_{1r} = y_1(y_2 + y_3y_4 + \cdots + y_{2r-1}y_{2r}),$$



$$\Psi_2 = y_1y_2y_3 + \bar{y}_1y_4y_5 \qquad (\bar{y}_1 = y_1 + 1),$$
$$\Psi_3 = y_1y_2y_6 + y_1y_3y_5 + y_2y_3y_4,$$
$$\Psi_4 = y_1y_2y_7 + y_1y_3y_4 + y_2y_5y_6.$$

其中当 $r = 1$ 时约记 $\Psi_{11} = y_1y_2$.

基于此定理便可进而推出

定理 G. 在三阶 RM 码中，重量 $k = 2^{m-2}$ 的码字个数等于

$$N_{m,k} = \sum_{i=1}^{4} N_i,$$

其中

$$N_1 = \sum_{k=1}^{[m/2]} |S_m(y_1(y_2 + y_3y_4 + \cdots + y_{2k-1}y_{2k}))|$$
$$= 2^2(2^m - 1)\left(2^{m(m-1)/2} - \sum_{j=0}^{[(m-1)/2]} 2^{j(j+1)} \times \frac{(2^{m-1}-1)(2^{m-2}-1)\cdots(2^{m-2j}-1)}{(4-1)(4^2-1)\cdots(4^j-1)} - \frac{2^3}{3}(2^m-1)(2^{m-1}-1)\right),$$

$$N_2 = |S_m(\Psi_2)| = (2^8/3^2)(2^m-1)(2^{m-1}-1)\cdots(2^{m-4}-1),$$
$$N_3 = |S_m(\Psi_3)| = (2^{10}/3)(2^m-1)(2^{m-1}-1)\cdots(2^{m-5}-1),$$
$$N_4 = |S_m(\Psi_4)| = (2^{15}/3^2)(2^m-1)(2^{m-1}-1)\cdots(2^{m-6}-1). \qquad (19)$$

而 $|S_m(f)|$ 如前表示与 f 相 A 等价的多项式个数.

作为对结果的一个验证，分别取 $m = 6, 7$：当 $m = 6$ 时，$N_1 = 2^2\cdot3\cdot5\cdot7\cdot31\cdot353$，$N_2 = 2^8\cdot3^2\cdot5\cdot7^2\cdot31$，$N_3 = 2^{10}\cdot2^3\cdot5\cdot7^2\cdot31$，$N_4 = 0$，故 $N_{m,k} = N_1 + N_2 + N_3 + N_4 = 2^2\cdot3\cdot5^3\cdot$



$7\cdot31^2\cdot23$; 当 $m=7$ 时, $N_1=2^2\cdot3\cdot5^2\cdot7\cdot127\cdot1741$, $N_2=2^8\cdot3\cdot5\cdot7^2\cdot31\cdot127$, $N_3=2^{10}\cdot3^3\cdot5\cdot7^2\cdot31\cdot127$, $N_4=2^{15}\cdot3^2\cdot5\cdot7^2\cdot31\cdot127$, 故 $N_{m,k}=N_1+N_2+N_3+N_4=2^2\cdot3^3\cdot5\cdot7\cdot11^2\cdot19\cdot127\cdot283$. 此与用电子计算机解出的已知结果一致. ($m=6$ 见 Sloane and Berlekamp [144], $m=7$ 见 Sugino *et al.*[149].) 由定理 G 还可以导出 $m=8$ 时的三阶 *RM* 码的重量分布, 这是迄今未获完全的重量分布的三阶 *RM* 码中, 参数最小的一组.

定理 D—G 的证明都比较长, 限于篇幅, 我们仅以(19)之证明为例说明推导的方式.

如前, 我们用 $|S_7(\Psi_4)|$ 表示可经变元的 A 变换

$$y_i=\sum_{j=1}^{7}\alpha_{ij}x_j+\alpha_{i0}\qquad(i=1,2,\cdots,7)\tag{20}$$

可化至 Ψ_4 的多项式 $f(x_1,\cdots,x_7)$ 个数, 而用 $|G_7(\Psi_4)|$ 表示使得 Ψ_4 不变的 A 变换(20)的个数. 仿(14)式之证易见

$$|S_m(\Psi_4)|=2^{28}(2^m-1)\cdots(2^{m-6}-1)/|G_7(\Psi_4)|.$$

故为证(19)式只需证明

命题 3. $|G_7(y_1y_2y_7+y_1y_3y_4+y_2y_5y_6)|=3^2\cdot2^{13}$.

证. 设

$$y_i'=\sum_{j=1}^{7}\alpha_{ij}y_j+\alpha_{i0}\qquad(i=1,\cdots,7)\tag{21}$$

使得 $\Psi_4=y_1y_2y_7+y_1y_3y_4+y_2y_5y_6$ 不变, 亦即

$$y_1y_2y_7+y_1y_3y_4+y_2y_5y_6=y_1'y_2'y_7'+y_1'y_3'y_4'+y_2'y_5'y_6'.\tag{22}$$

比较两边 $y_iy_6y_7$ $(i=1,2,\cdots,5)$ 前系数可得

$$\alpha_{1i}\left(\begin{vmatrix}\alpha_{26}&\alpha_{27}\\\alpha_{76}&\alpha_{77}\end{vmatrix}+\begin{vmatrix}\alpha_{36}&\alpha_{37}\\\alpha_{46}&\alpha_{47}\end{vmatrix}\right)+\alpha_{2i}\left(\begin{vmatrix}\alpha_{16}&\alpha_{17}\\\alpha_{76}&\alpha_{77}\end{vmatrix}\right.$$

$$\left.+\begin{vmatrix}\alpha_{56}&\alpha_{57}\\\alpha_{66}&\alpha_{67}\end{vmatrix}\right)+\alpha_{3i}\begin{vmatrix}\alpha_{16}&\alpha_{17}\\\alpha_{46}&\alpha_{47}\end{vmatrix}+\alpha_{4i}\begin{vmatrix}\alpha_{16}&\alpha_{17}\\\alpha_{36}&\alpha_{37}\end{vmatrix}$$



$$+\alpha_{5i}\begin{vmatrix}\alpha_{26}&\alpha_{27}\\\alpha_{66}&\alpha_{67}\end{vmatrix}+\alpha_{6i}\begin{vmatrix}\alpha_{26}&\alpha_{27}\\\alpha_{56}&\alpha_{57}\end{vmatrix}$$

$$+\alpha_{7i}\begin{vmatrix}\alpha_{16}&\alpha_{17}\\\alpha_{26}&\alpha_{27}\end{vmatrix}=0.$$

因当 $i=6,7$ 时上式同样成立，故上式对 $i=1,2,\cdots,7$ 均成立，于是由变换(21)的非奇性，$\det(\alpha_{ij})\neq 0$，可见

$$\begin{vmatrix}\alpha_{16}&\alpha_{17}\\\alpha_{46}&\alpha_{47}\end{vmatrix}=\begin{vmatrix}\alpha_{16}&\alpha_{17}\\\alpha_{36}&\alpha_{37}\end{vmatrix}=\begin{vmatrix}\alpha_{26}&\alpha_{27}\\\alpha_{66}&\alpha_{67}\end{vmatrix}$$

$$=\begin{vmatrix}\alpha_{26}&\alpha_{27}\\\alpha_{56}&\alpha_{57}\end{vmatrix}=\begin{vmatrix}\alpha_{16}&\alpha_{17}\\\alpha_{26}&\alpha_{27}\end{vmatrix}=0.$$

用类似的推理可证：若 $\{r,s\}$ 非 $\{1,3,4\}$，$\{1,2,7\}$，$\{2,5,6\}$ 中任一的子集，则

$$\begin{vmatrix}\alpha_{ir}&\alpha_{is}\\\alpha_{jr}&\alpha_{js}\end{vmatrix}=0$$

$$((i,j)=(1,2),(1,3),(1,4),(2,5),(2,6)).\tag{23}$$

今若 $\alpha_{17}=1$，则由

$$\begin{vmatrix}\alpha_{13}&\alpha_{17}\\\alpha_{i3}&\alpha_{i7}\end{vmatrix}=\begin{vmatrix}\alpha_{14}&\alpha_{17}\\\alpha_{i4}&\alpha_{i7}\end{vmatrix}=\begin{vmatrix}\alpha_{15}&\alpha_{17}\\\alpha_{i5}&\alpha_{i7}\end{vmatrix}$$

$$=\begin{vmatrix}\alpha_{16}&\alpha_{17}\\\alpha_{i6}&\alpha_{i7}\end{vmatrix}=0\quad(i=2,3,4)$$

可见阵

$$A=\begin{bmatrix}\alpha_{13}&\alpha_{14}&\alpha_{15}&\alpha_{16}&\alpha_{17}\\\alpha_{23}&&\cdots\cdots\cdots&&\alpha_{27}\\\alpha_{33}&&\cdots\cdots\cdots&&\alpha_{37}\\\alpha_{43}&&\cdots\cdots\cdots&&\alpha_{47}\end{bmatrix}$$

之秩数为 1，此不可能。(因由 Laplace 展开定理易证，一个 7 阶非奇阵不可能有 4×5 阶秩为 1 的子阵。)因而 $\alpha_{17}=0$，同



理 $\alpha_{27}=0$.

又若 $\alpha_{13}=1$，则由

$$\begin{vmatrix}\alpha_{17} & \alpha_{13}\\ \alpha_{i7} & \alpha_{i3}\end{vmatrix}=\begin{vmatrix}\alpha_{16} & \alpha_{13}\\ \alpha_{i6} & \alpha_{i3}\end{vmatrix}=\begin{vmatrix}\alpha_{15} & \alpha_{13}\\ \alpha_{i5} & \alpha_{i3}\end{vmatrix}$$

$$=\begin{vmatrix}\alpha_{12} & \alpha_{13}\\ \alpha_{i2} & \alpha_{i3}\end{vmatrix}=0 \quad (i=2,3,4),$$

可见阵

$$\begin{bmatrix}\alpha_{12} & \alpha_{13} & \alpha_{15} & \alpha_{16} & \alpha_{17}\\ \alpha_{22} & \cdots & \cdots & & \alpha_{27}\\ \alpha_{32} & & \cdots & \cdots & \alpha_{37}\\ \alpha_{42} & \cdots & & \cdots & \alpha_{47}\end{bmatrix}$$

之秩数为 1，此同样不可能．故 $\alpha_{13}=0$．由对称性相仿可证

$$\alpha_{14}=\alpha_{15}=\alpha_{16}=\alpha_{23}=\alpha_{24}=\alpha_{25}=\alpha_{26}=0.$$

同样，若 $\alpha_{37}=1$，则由

$$\begin{vmatrix}\alpha_{33} & \alpha_{37}\\ \alpha_{43} & \alpha_{47}\end{vmatrix}=\begin{vmatrix}\alpha_{34} & \alpha_{37}\\ \alpha_{44} & \alpha_{47}\end{vmatrix}=\begin{vmatrix}\alpha_{35} & \alpha_{37}\\ \alpha_{45} & \alpha_{47}\end{vmatrix}=\begin{vmatrix}\alpha_{36} & \alpha_{37}\\ \alpha_{46} & \alpha_{47}\end{vmatrix}=0,$$

可见 $(\alpha_{33},\alpha_{34},\alpha_{35},\alpha_{36},\alpha_{37})$ 与 $(\alpha_{43},\alpha_{44},\alpha_{45},\alpha_{46},\alpha_{47})$ 相关．因已证得 $\alpha_{1i}=\alpha_{2i}=0 \quad (i=3,4,\cdots,7)$，故又将得出阵 $\boldsymbol{A}$ 之秩数等于 1，此不可能，故 $\alpha_{37}=0$．由对称性同样可证 $\alpha_{47}=\alpha_{57}=\alpha_{67}=0$．综合所得，即有

$$\begin{aligned}\alpha_{1j}=\alpha_{2j}&=0 \qquad (j=3,4,5,6,7),\\ \alpha_{i7}&=0 \qquad (i=3,4,5,6).\end{aligned} \tag{24}$$

再由阵 (α_{ij}) 非奇，即见

$$\begin{vmatrix}\alpha_{11} & \alpha_{12}\\ \alpha_{21} & \alpha_{22}\end{vmatrix}=\begin{vmatrix}\alpha_{33} & \alpha_{34} & \alpha_{35} & \alpha_{36}\\ \alpha_{43} & \cdots & \cdots & \alpha_{46}\\ \alpha_{53} & \cdots & \cdots & \alpha_{56}\\ \alpha_{63} & \cdots & \cdots & \alpha_{66}\end{vmatrix}=\alpha_{77}=1. \tag{25}$$



由$\begin{vmatrix} \alpha_{11} & \alpha_{15} \\ \alpha_{31} & \alpha_{35} \end{vmatrix} = 0$ 及 $\alpha_{15} = 0$ 得 $\alpha_{11}\alpha_{35} = 0$，相仿讨论可得

$$\begin{aligned} &\alpha_{11}\alpha_{35} = \alpha_{11}\alpha_{45} = \alpha_{11}\alpha_{36} = \alpha_{11}\alpha_{46} = 0, \\ &\alpha_{12}\alpha_{33} = \alpha_{12}\alpha_{43} = \alpha_{12}\alpha_{34} = \alpha_{12}\alpha_{44} = 0, \\ &\alpha_{21}\alpha_{55} = \alpha_{21}\alpha_{65} = \alpha_{21}\alpha_{56} = \alpha_{21}\alpha_{66} = 0, \\ &\alpha_{22}\alpha_{53} = \alpha_{22}\alpha_{63} = \alpha_{22}\alpha_{54} = \alpha_{22}\alpha_{64} = 0. \end{aligned} \tag{26}$$

今设 $\alpha_{11} = 1$（当 $\alpha_{12} = 1$ 时，由对称性，讨论相仿）．此时由(26)得$\begin{bmatrix} \alpha_{35} & \alpha_{36} \\ \alpha_{45} & \alpha_{46} \end{bmatrix} = 0$，故由(25)得$\begin{vmatrix} \alpha_{33} & \alpha_{34} \\ \alpha_{43} & \alpha_{44} \end{vmatrix} = \begin{vmatrix} \alpha_{55} & \alpha_{56} \\ \alpha_{65} & \alpha_{66} \end{vmatrix} = 1$．于是 α_{33}，α_{34} 以及 α_{55}，α_{65} 中至少有一个 $\neq 0$．再由(26)得见 $\alpha_{12} = \alpha_{21} = 0$，由此 $\alpha_{22} = \begin{vmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{vmatrix} = 1$．复由(26)得$\begin{vmatrix} \alpha_{53} & \alpha_{54} \\ \alpha_{63} & \alpha_{64} \end{vmatrix} = 0$．综合所得即有

$$\begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

$$\begin{vmatrix} \alpha_{33} & \alpha_{34} \\ \alpha_{43} & \alpha_{44} \end{vmatrix} = \begin{vmatrix} \alpha_{55} & \alpha_{56} \\ \alpha_{65} & \alpha_{66} \end{vmatrix} = 1,$$

$$\begin{bmatrix} \alpha_{35} & \alpha_{36} \\ \alpha_{45} & \alpha_{46} \end{bmatrix} = \begin{bmatrix} \alpha_{53} & \alpha_{54} \\ \alpha_{63} & \alpha_{64} \end{bmatrix} = 0. \tag{27}$$

今证 $\alpha_{10} = 0$．不然若 $\alpha_{10} = 1$，则 $y_1' = \bar{y}_1$，从而 $y_1y_2y_7\Psi' = y_1y_2y_7(y_2'y_5'y_6')$（这里 $\Psi' = y_1'y_2'y_7' + y_1'y_3'y_4' + y_2'y_5'y_6'$），此不可能．因可证 $|y_1y_2y_7\Psi'|_m = 2^{m-4} + 2^{m-6}$，而 $|y_1y_2y_7y_2'y_5'y_6'|_m$ 必为 2 的幂次，两者不可能相等．实际上，一方面 $|y_1y_3y_4 + y_2y_5y_6|_m = |y_1y_3y_4|_m + |y_2y_5y_6|_m - 2|y_1y_3y_4y_2y_5y_6|_m = 2^{m-3} + 2^{m-3} - 2\cdot 2^{m-6} = 2^{m-2} - 2^{m-5}$；另一方面 $|y_1y_3y_4 + y_2y_5y_6|_m = |y_1y_2y_7 + \Psi'|_m = |y_1y_2y_7|_m + |\Psi'|_m - 2|y_1y_2y_7\Psi'|_m = 2^{m-3} +$



$2^{m-2}-2|y_1y_2y_7\Psi'|_m$，故 $|y_1y_2y_7\Psi'|_m=(1/2)((2^{m-3}+2^{m-2})-(2^{m-2}-2^{m-5}))=2^{m-4}+2^{m-6}$. 由上述矛盾知 $\alpha_{10}=0$. 同理可证 $\alpha_{20}=0$.

再比较(22)式两边 $y_1y_2y_i\ (i=3, 4, 5, 6)$ 前系数可得

$$\alpha_{73}=\begin{vmatrix}\alpha_{32} & \alpha_{33}\\ \alpha_{42} & \alpha_{43}\end{vmatrix},\quad \alpha_{74}=\begin{vmatrix}\alpha_{32} & \alpha_{34}\\ \alpha_{42} & \alpha_{44}\end{vmatrix},$$
$$\alpha_{75}=\begin{vmatrix}\alpha_{51} & \alpha_{53}\\ \alpha_{61} & \alpha_{63}\end{vmatrix},\quad \alpha_{76}=\begin{vmatrix}\alpha_{51} & \alpha_{56}\\ \alpha_{61} & \alpha_{66}\end{vmatrix}. \tag{28}$$

比较 y_1y_3 与 y_1y_4 前系数可得

$$\begin{vmatrix}\alpha_{33} & \alpha_{30}+\alpha_{31}\\ \alpha_{43} & \alpha_{40}+\alpha_{41}\end{vmatrix}=\alpha_{33}\alpha_{43},\quad \begin{vmatrix}\alpha_{34} & \alpha_{30}+\alpha_{31}\\ \alpha_{44} & \alpha_{40}+\alpha_{41}\end{vmatrix}=\alpha_{34}\alpha_{44}.$$

注意到$\begin{vmatrix}\alpha_{33} & \alpha_{43}\\ \alpha_{34} & \alpha_{44}\end{vmatrix}=1$，由上两式联立便可解出

$$\alpha_{30}+\alpha_{31}=\begin{vmatrix}\alpha_{33} & \alpha_{33}\alpha_{43}\\ \alpha_{34} & \alpha_{34}\alpha_{44}\end{vmatrix}=\alpha_{33}\alpha_{34}(\alpha_{43}+\alpha_{44}),$$
$$\alpha_{40}+\alpha_{41}=\begin{vmatrix}\alpha_{33}\alpha_{43} & \alpha_{43}\\ \alpha_{34}\alpha_{44} & \alpha_{44}\end{vmatrix}=\alpha_{43}\alpha_{44}(\alpha_{33}+\alpha_{34}). \tag{29}$$

但 α_{33}, α_{34} 不全为零,因而 $\alpha_{33}\alpha_{34}=1+\alpha_{33}+\alpha_{34}$, 同理 $\alpha_{33}\alpha_{43}=1+\alpha_{33}+\alpha_{43}$, $\alpha_{34}\alpha_{44}=1+\alpha_{34}+\alpha_{44}$, 代入(29)式便可得出 $\alpha_{30}+\alpha_{31}=1+\alpha_{33}+\alpha_{34}$.同理可得 $\alpha_{40}+\alpha_{41}=1+\alpha_{43}+\alpha_{44}$. 再比较(22)式两边 y_2y_5 及 y_2y_6 前系数,同样方式可推知 α_{50}, α_{60} 之表式. 合写在一起即

$$\begin{aligned}\alpha_{30}&=1+\alpha_{31}+\alpha_{33}+\alpha_{34},\\ \alpha_{40}&=1+\alpha_{41}+\alpha_{43}+\alpha_{44},\\ \alpha_{50}&=1+\alpha_{52}+\alpha_{55}+\alpha_{56},\\ \alpha_{60}&=1+\alpha_{62}+\alpha_{65}+\alpha_{66}.\end{aligned} \tag{30}$$

又比较(22)式两边 y_1y_2 前系数可得



$$\alpha_{70}=\begin{vmatrix}\alpha_{32} & \alpha_{30}\\ \alpha_{42} & \alpha_{40}\end{vmatrix}+\begin{vmatrix}\alpha_{51} & \alpha_{50}\\ \alpha_{61} & \alpha_{60}\end{vmatrix}$$
$$+\alpha_{71}+\alpha_{72}+\alpha_{31}\alpha_{42}+\alpha_{32}\alpha_{41}$$
$$+\alpha_{32}\alpha_{42}+\alpha_{52}\alpha_{61}+\alpha_{51}\alpha_{61}+\alpha_{51}\alpha_{62}.$$

将(30)式代入

$$\alpha_{70}=\bar{\alpha}_{32}\bar{\alpha}_{42}+\bar{\alpha}_{51}\bar{\alpha}_{61}+\begin{vmatrix}\alpha_{32} & \alpha_{33}+\alpha_{34}\\ \alpha_{42} & \alpha_{43}+\alpha_{44}\end{vmatrix}+\begin{vmatrix}\alpha_{51} & \alpha_{55}+\alpha_{56}\\ \alpha_{61} & \alpha_{65}+\alpha_{66}\end{vmatrix}. \quad (31)$$

综合所得,即见变换(21)形如

$$\begin{cases}y_1'= y_1,\\ y_2'= y_2,\\ y_3'=1+\alpha_{31}\bar{y}_1+\alpha_{32}y_2+\alpha_{33}\bar{y}_3+\alpha_{34}\bar{y}_4,\\ y_4'=1+\alpha_{41}\bar{y}_1+\alpha_{42}y_2+\alpha_{43}\bar{y}_3+\alpha_{44}\bar{y}_4,\\ y_5'=1+\alpha_{51}y_1+\alpha_{52}\bar{y}_2+\alpha_{55}\bar{y}_5+\alpha_{56}\bar{y}_6,\\ y_6'=1+\alpha_{61}y_1+\alpha_{62}\bar{y}_2+\alpha_{65}\bar{y}_5+\alpha_{66}\bar{y}_6,\\ y_7'=\alpha_{71}\bar{y}_1+\alpha_{72}\bar{y}_2+\begin{vmatrix}\alpha_{32} & \alpha_{33}\\ \alpha_{42} & \alpha_{43}\end{vmatrix}\bar{y}_3+\begin{vmatrix}\alpha_{32} & \alpha_{34}\\ \alpha_{42} & \alpha_{44}\end{vmatrix}\bar{y}_4\\ \qquad+\begin{vmatrix}\alpha_{51} & \alpha_{55}\\ \alpha_{61} & \alpha_{65}\end{vmatrix}\bar{y}_5+\begin{vmatrix}\alpha_{51} & \alpha_{56}\\ \alpha_{61} & \alpha_{66}\end{vmatrix}\bar{y}_6+y_7\\ \qquad+(\bar{\alpha}_{32}\bar{\alpha}_{42}+\bar{\alpha}_{51}\bar{\alpha}_{61}),\end{cases}$$

以及 $y_1'=y_2$, $y_2'=y_1$ 时相应的形式。在此种变换中,α_{i1}, α_{i2} $(i=3,4,\cdots,7)$ 可自由选择;而 α_{33}, α_{43}, α_{34}, α_{44} 应选择使得$\begin{vmatrix}\alpha_{33} & \alpha_{34}\\ \alpha_{43} & \alpha_{44}\end{vmatrix}=1$,故有 $(2^2-1)(2^2-2)=6$ 种取法。同样,α_{55}, α_{56}, α_{65}, α_{66} 也有 6 种取法。再注意到$\begin{vmatrix}\alpha_{11} & \alpha_{12}\\ \alpha_{21} & \alpha_{22}\end{vmatrix}$有 $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ 及 $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$ 两种取法,可见使得 Ψ_4 不变的变换



(22)之个数为

$$|G_7(y_1y_2y_7 + y_1y_3y_4 + y_2y_5y_6)|$$
$$= 2 \times 6^2 \times 2^{10} = 3^2 \times 2^{13}.$$

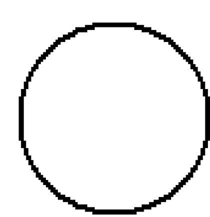
证毕。

因 $|f+1|_m = 2^m - |f|_m$，故由上述定理可见，为了定出三阶 RM 码的完全的重量分布，我们尚须求出当 f 的重量满足

$$2^{m-2} < |f|_m < 2^{m-1}$$

时相应三次多项式的分类及每个类中元的个数．这是一个迄今未决的问题，任何这方面的进一步结果无疑是很有价值的．

关于其它码类的重量分布问题，迄今对所谓自对偶码的研究居多(见 Berlekamp *et al.* [38], MacWilliams *et al.* [108], Malloms and Sloane [109])，因为此时码字的重量分布有某种确定的不变性．另外，对应用很广泛的 BCH 码的重量分布问题，也有不少工作，特别是 Сидельников 在[54]中证得，BCH 码的重量分布函数在极限状态即为正态分布．有关这方面的结果，在此就不再详述了．





第六章　计算机算法

6.1. 两种遍数性质的算法

在运筹学等各个应用数学分支中，有一大部分搜索问题和极值问题可叙述成下面的形式：给出一个有限集合 $X = \{x_1, x_2, \cdots, x_m\}$，要求找出 X 中的一个(或者所有)具某种特定性质的元 x_i。这里的"特定性质"可以是 x_i 应满足的一组条件，也可以是使得某个目标函数 $f(x)$ 达到极值。前者泛称为搜索问题，后者泛称为优化问题。

对于搜索问题，最直捷了当的解法自然是逐个检验各 x_i，看是否满足所述条件？将满足条件的诸元逐一筛选出来，对于优化问题也相仿。例如要求使 $f(x)$ 达最小值，先求出 $f(x_1)$，然后求出 $f(x_2)$，两者比较留下较小的一个，再与 $f(x_3)$ 比较，如此反复。这种最原始的遍数性质的算法虽然简单，但因要求遍访 X 中的每个元，工作量之大常常无法付诸实现。因为一般 $|X|$ 的数量级常与 $n!$ 或 m^n (甚至 n^n) 相当，当 n 增大时，$n!$ 或 m^n 急剧增长，即使 n 不大，$n!$，m^n 也已如天文数字之巨。例如 $50! \approx 3 \times 10^{56} \times 10^8$，$100! \approx 10^{150} \times 10^8$。即使是现代最高速的每秒可运算上亿($10^8$)次的电子计算机也对之自叹莫如。由于这一原因，人们努力寻求各种能结合具体问题的特点来求解的更有效的算法。近年来，随着计算机算法研究的深入，也的确提出了许多行之有效的算法。但尽管如此，遍数性质的算法依然占有相当重要的地位。这是由于实践中遇到的问题通常很复杂，有许多问题



迄今仍无行之有效的算法（有些问题甚至可以证明不存在一种“有效的”算法），仍需仰仗于遍数性质的算法．此外，我们在研究某个问题或探索某种算法的初期，也常常需要引用遍数性质的算法所得出的结果作为印证，因此有必要研讨某种遍数的技巧．本节介绍的“顺路返回”算法与“分枝定界”算法就属于这种遍数性质的算法．前者用于求解搜索问题，后者用于求解优化问题．

“顺路返回”算法与“分枝定界”算法的共同特点是设法赋予集合 X 以一种树形结构，如图 1 所示．树中的每个“叶点” $a, b, c, \cdots$ 对应于集合 X 中的各个元 x_i．在算法进行的过程中，我们从树的“根点” o 出发，沿着某个分枝往下走．每

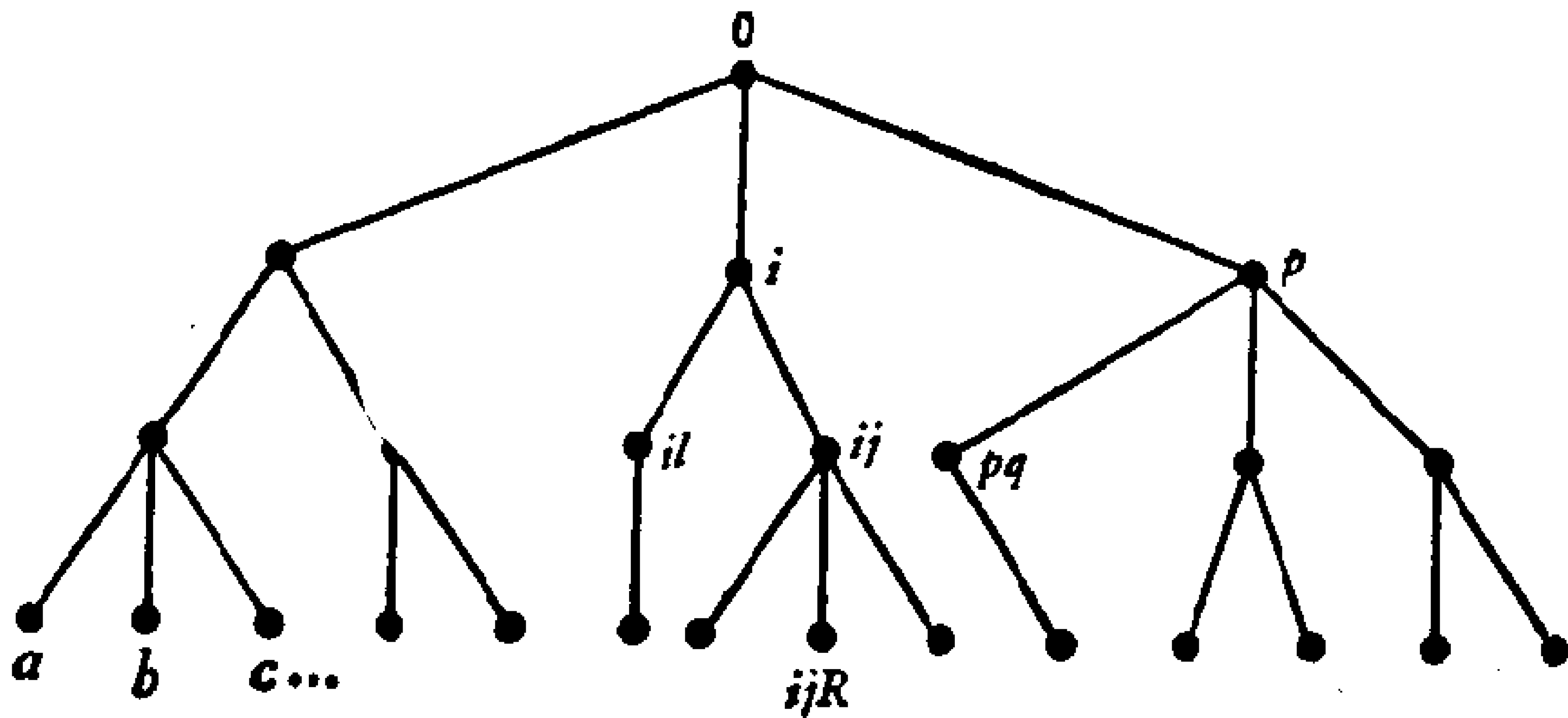


图 1．

到达一个分枝点，我们面临数个分枝可供继续前进时的选择．此时我们必须作出某种判断，选择一枝“印象”较好的分枝继续前进，或者认定继续前进已无必要，返回到前面的某个分枝点，从该点开始沿另一分枝前进．如此反复，直至找到一个符合要求的“叶点”为止．

6.1.1. “顺路返回”算法

这一算法的目标是找出集合 X 中满足某种条件的所有元．在算法的进行过程中，每到达一个分枝点 $(ij\cdots kl)$，我



们根据条件的要求，列出能够继续前进的所有分枝 $(ij\cdots kls_1)$, $(ij\cdots kls_2)$, $\cdots$，从中任取一枝前进。当这种分枝不存在时，则顺着来路返回到前一分枝点 $(ij\cdots k)$，再从该点沿另一分枝 $(ij\cdots kl')$ 摸索前进。一旦抵达某个叶点 $(a_1, a_2\cdots a_{n-1}a_n)$ 后，记下与之相应的 $x\in X$，然后再顺路返回到前一分枝点 $(a_1a_2\cdots a_{n-1})$，选择合乎条件的另一分枝（如果没有这种分枝，则再往上溯），如此反复，直到"山穷水尽已无路"才罢休。

这种遍数技巧与不假思索地遍访每个元 $x\in X$ 的最原始的算法相比，其优点在于：它使我们能早期识别出一类不满足条件的元，用不着辛辛苦苦走到叶点才发现走错了路。这样，在某个分枝点 $(a_1a_2\cdots a_k)$ 就能及早回头，不用再去拜访形如 $(a_1a_2\cdots a_ka'_{k+1}\cdots a'_n)$ 的所有叶点，省去了不少的工作量。

在设计相应的计算机算法时，我们将每个叶点表示成 $(A(1), A(2), \cdots, A(n))$ 的形式，于是每个部分向量 $(A(1), \cdots, A(k))$ 便表示一个分枝点。每到一个分枝点 $(A(1), \cdots, A(k-1))$，我们首先求出可选作 $A(k)$ 的所有值 $i_1, \cdots, i_q$，并将这些值连同其个数 q 存放在一个栈中（图 2）。然后取出栈中最后一个元 $S(l)=q$，它指出了可选作 $A(k)$ 的值的个数。若 $q\neq 0$，则取出 $S(l-1)$ 作为

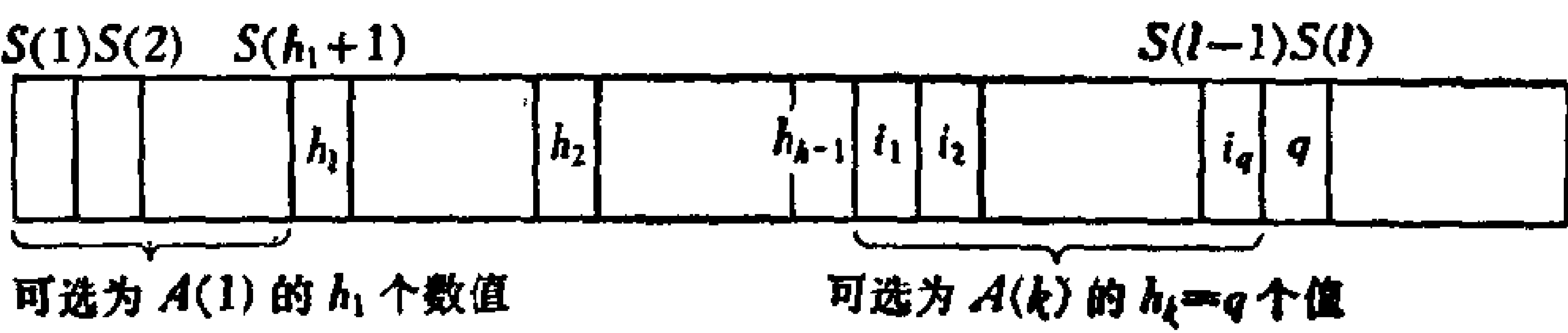


图 2. 栈的形式

$A(k)$ 并将 q 减 1 送到已空出的位置 $S(l-1)$ 中。若 $q=0$,



则继续取 $S(l-1)$ 中存放的 $A(k-1)$ 个数，重复上述过程，直至获得一个完整的向量 $(A(1),\cdots,A(n))$，输出后继续上述过程.

下面我们以图的染色为例，说明这一算法的执行方式.

设 G 为一 n 个点的图，$C=\{1,2,\cdots,p\}$ 为 p 种色组成的色集合. 若将 G 的每个点 i 染以色 $c_i\in C$，使得图中相邻的点具不同的色，则称此种染色方式为适当的染色. 图 3 表出了一个图的适当染色与不适当染色.

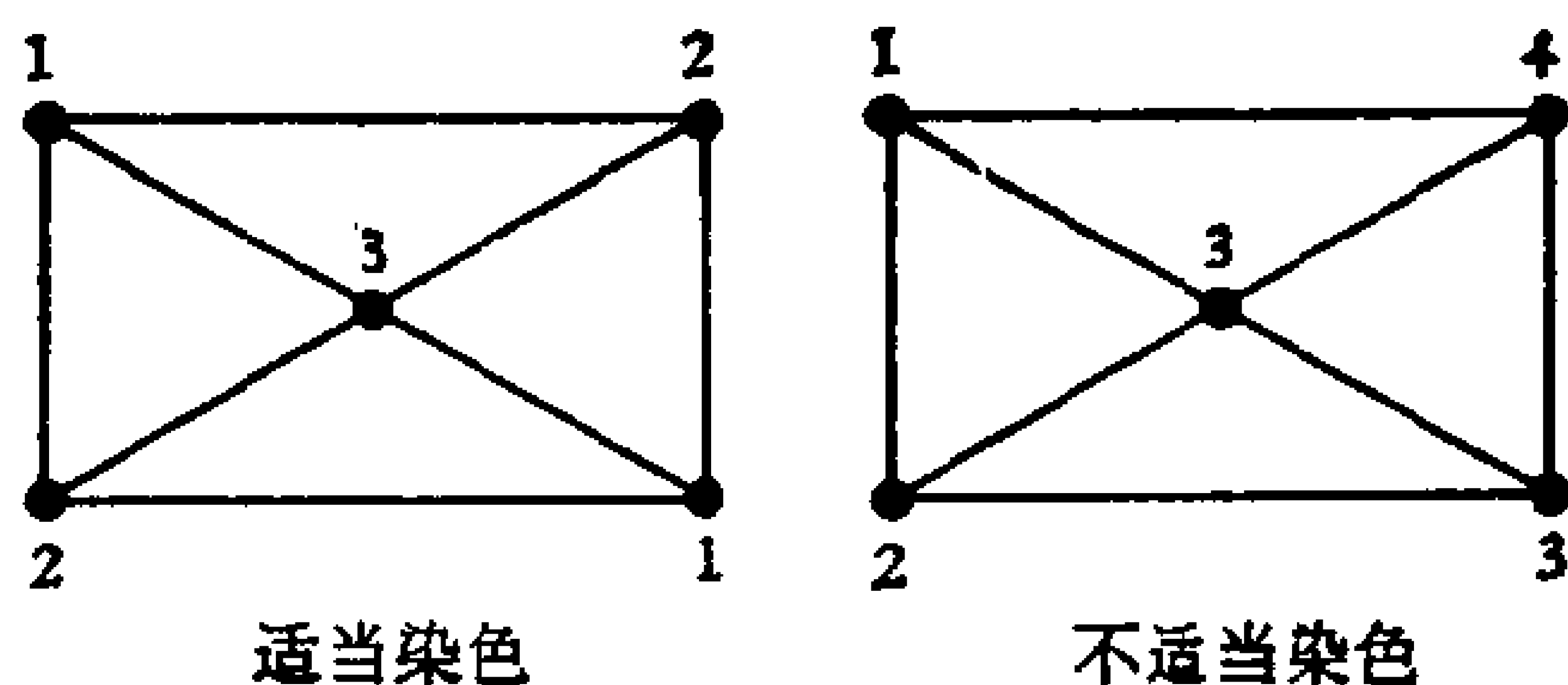


图 3. 适当染色与不适当染色

今用顺路返回算法求出图 G 的各种适当染色的方式. 为此假设图 G 由下面的矩阵 $A=(a_{ij})$ 给出:

$$a_{ij}=\begin{cases}1, & \text{若点 } i \text{ 和 } j \text{ 在 } G \text{ 中相邻;}\\ 0, & \text{若点 } i \text{ 和 } j \text{ 在 } G \text{ 中不相邻.}\end{cases}$$

又以 $C(i)$ 表示点 i 的染色，此时相应的树形图的每一分枝点对应于图 G 的一种部分染色方式 $(C(1),C(2),\cdots,C(k))$. 作为规格化的染色方式，我们取定 $C(1)=1$，亦即各种染色方式均将点 1 染以同一色 1. 由问题的要求可知，在到达某个分枝点 $(C(1),C(2),\cdots,C(k-1))$ 后，满足下列条件的任一色 i 均可取作第 k 点的色 $C(k)$:

(i) $1\leqslant i\leqslant p$; (ii) $i\neq C(j)$，其中 $1\leqslant j\leqslant k-1$，且 $a_{jk}=1$.



下面是相应的算法，其中 A 为主程序部分，B 为子程序部分；$C(k)$，$a(i,j)$ 的意义见前，$S(i)$ 表示栈中第 i 个位置的内容，l 表示栈的当前长度．另外用 $w(i)$ 表示色 i 的特征值：$w(i)=1$ 表明色 i 可以选用，$w(i)=0$ 表明色 i 禁用．

染色算法 B．（选出 $C(k)$ 的各种可行值并存入栈中．）

$B1$．若 $k=1$ 去 $B2$，否则去 $B3$．

$B2$．$1\to S(1)$，$S(2)$，$2\to l$，返回（主程序 A）．

$B3$．对 $i=1,2,\cdots,p$，$1\to w(i)$．

$B4$．对 $i=1,2,\cdots,k-1$，完成 $B5$．

$B5$．若 $a(i,k)=1$，则 $0\to w(C(i))$；若 $a(i,k)=0$，不做工作．

$B6$．$l\to M$．

$B7$．对于 $i=1,2,\cdots,p$ 完成 $B8$．

$B8$．若 $w(i)=1$，则 $l+1\to l$，$i\to S(l)$；若 $w(i)=0$，不做工作．

$B9$．$l-M\to S(l+1)$，$l+1\to l$．

$B10$．返回．

说明．$B1$：判别是否算法开始？

$B2$：形成栈中初始量，$S(1)=C(1)=1$，$S(2)=h_1=1$ 及栈的当前长度 $l=2$．

$B3$—$B5$：将与点相邻的点 i 上已染之色 $C(i)$ 列为禁用．

$B6$—$B8$：将可用之色存中栈中 $S(l+1)$，$S(l+2)$，$\cdots$，$S(l+q)$ 处；修改栈的长度 $l+q\to l$．

$B9$：将新存入栈的色的个数 q 存入 $S(l+1)$，修改栈的长度 $l+1\to l$．



A.（主程序）.

$A1$. $1 \to k$, $0 \to l$.

$A2$. 转子程序 B.

$A3$. $S(l) \to q$, $l - 1 \to l$.

$A4$. 若 $q = 0$, 去 $A5$; 否则去 $A7$.

$A5$. $k - 1 \to k$.

$A6$. 若 $k = 0$, 算法执行完毕; 否则去 $A3$.

$A7$. $S(l) \to C(k)$, $q - 1 \to S(l)$.

$A8$. 若 $k = n$, 去 $A9$; 否则去 $A10$.

$A9$. 输出 $C(1), C(2), \cdots, C(n)$, 去 $A3$.

$A10$. $k + 1 \to k$, 去 $A2$.

说明. $A1$: 形成初始值.

$A2$: 转子,形成本次 $C(k)$ 的可行值.

$A3, A4$: 判本次可行值个数 q 是否为零?

$A5, A6$: 若 $q = 0$, 则返回上一分枝点.（当上一分枝点编号为 0 时,算法结束.）

$A7$: 若 $q \neq 0$, 取出一个可行值.

$A8, A9$: 是否到达“叶点”? 若是输出结果,否则 $k + 1$, 去下一分枝点.

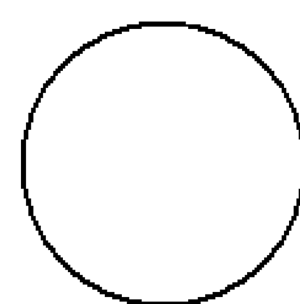
下面是用初级会话语言 *BASIC* 书写的程序.

```
10 REM COLORING THE VERTICES OF A GRAPH
12 READ P, N
14 DIM W(P), C(N), A(N,N), S((P + 1) * N)
16 FOR I = 1 TO N - 1
18         FOR J = I + 1 TO N
20             READ A(I, J)
22         NEXT J
24 NEXT I
```




```
26 LET K = 1
28 LET L = 0
30 GOSUB 100
32 LET Q = S(L)
34 LET L = L - 1
36 IF Q GOTO 44
38 LET K = K - 1
40 IF K GOTO 32
42 GOTO 300
44 LET C(K) = S(L)
46 LET S(L) = Q - 1
48 IF K - N GOTO 60
50 FOR I = 1 TO N
52          PRINT C(I);
54 NEXT I
56 PRINT
58 GOTO 32
60 LET K = K + 1
62 GOTO 30

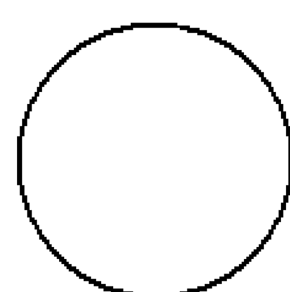
100 REM SUBROUTINE
102 IF K - 1 GOTO 112
104 LET S(1) = 1
106 LET S(2) = 1
108 LET L = 2
110 RETURN
112 FOR I = 1 TO P
114          LET W(I) = 1
```





```
116 NEXT I
118 FOR I = 1 TO K - 1
120       IF A(I, K) = 0 GOTO 124
122       LET W(C(I)) = 0
124 NEXT I
126 LET M = L
128 FOR I = 1 TO P
130       IF W(I) - 1 GOTO 136
132       LET L = M + 1
134       LET S(M) = I
136 NEXT I
138 LET S(M + 1) = M - L
140 LET L = M + 1
142 RETURN

200 DATA P, N
202 DATA A(1, 2), A(1, 3), ···, A(1, N),
         A(2, 3), ···, A(N - 1, N)
```



```
300 END
```

最后顺便一提的是，图的染色问题是图论中所研究的一个重要课题，它在日程表安排、逻辑线路故障检查等实践问题中都有应用（见 Akers[20]，Cadogan [46]，Garey [66]，Neufeld, *et al.* [117]）．在理论方面，则有著名的**“四色猜测”**：每个平面图都可以用四种色使图中各点适当地染色．所谓平面图是指可以在平面上画出来，使得各条边互不相交的一种图，“四色猜测”在数学史上极为有名，Ore 在 [122] 中曾将此猜测与数论中的 Fermat 大定理及 Riemann 假设并提为三大数学



难题．这一问题从大约 1852 年提出至今悬而未决达一百二十余年（见 Saaty [140]），直至最近，Appel[24] 与 Appel and Haken[25] 才宣称：他们借助于现代高速电子计算机最终证明了四色猜测的正确性，为此花了近二千个计算机小时．四色猜测长期以来得不到解决的原因之一是所需讨论分析的对象其数量极为浩繁，在作者看来，Heesch [85] 的出现在解决四色猜测方面是一大转折点．Heesch 第一次展示了用计算机得出的一大批“可约结构”，指出了用计算机解决四色问题的巨大可能性．所谓可约结构乃指四色猜测的一个点数最少的反例图中不可能出现的一类图形．多年来不少数学家致力于寻求各种可约结构，以图最后证明：每个平面图至少包含一个可约结构，由此便可推出四色猜测的正确性．但由于一个可约结构的导出，需检查并分析各种可能情形，论证极为细致，当可约结构中点数增多时，工作量极大，因而自 Birkhoff 起虽经不少数学家的努力，积累了相当数量的可约结构，但其数量离开证明“每个平面图都包含一个可约结构”还极为遥远．直至 Heesch 的工作指明用设计计算机算法寻求可约结构后，方使这种努力面目一新．由此例可见，计算机算法的设计与研究，在现代数学的各个研究领域中，正在起着越来越重要的作用．

“顺路返回”算法系 Lehmer 在[100]中首先提出的，在各类组合结构的遍数方面已有很多应用，关于这方面的工作可见 Golomb and Baumert [69]，Knuth [99]，Schmidt and Druffel [142] 及 Dénes and Keedwell [55]，Nijenhuis [118] 等．

6.1.2. 分枝定界算法

分枝定界算法是 Little 在 [103] 中为解决著名的“货郎担”问题首先提出的，现已在各种运筹学问题中有了很多应用．假设我们需求得 $\min_x f(x)$ 的极小点 x．分枝定界算法的基本思想是：每到达一个分枝点 $(ij\cdots k)$，设法定出此后各个分枝 $(ij\cdots kl_1), (ij\cdots kl_2), \cdots$ 上目标函数 $f(x)$ 的下界，从中选择一个下界最小的分枝继续前进．因为我们设想：沿



下界小的分枝找到最小值点的可能性似乎大些．重复这种分枝定界的过程，便可到达某个叶点x'．此时，将$f(x')$的值与各个分枝点上已定出的下界相比较，若各分枝点的下界值都$\geqslant f(x')$，则$f(x')$便是最小值；否则选择一个下界最小的分枝重复上述过程．由此可见，运用分枝定界算法的两个主要步骤是：(i) 赋予集合X以某种树形结构，亦即分枝的方法；(ii) 在每个分枝点上给出一个较好的下界，亦即定界的方法．

下面我们以**零件加工顺序问题**（见越民义、韩继业 [9] [10]）说明分枝定界算法的实现方式．

设有n个零件$J_1, J_2, \cdots, J_n$须在m台机床$M_1, \cdots, M_m$上加工．假定每个零件J_j都需依次通过$M_1, M_2, \cdots, M_m$，又假定每台机床上在同一时间只能加工一种零件，且诸零件以同一顺序$J_{i_1}, J_{i_2}, \cdots, J_{i_n}$经过各个机床$M_k$，这里$\omega=(i_1, i_2, \cdots, i_n)$是$1, 2, \cdots, n$的一个排列．假设在$M_i$上加工$J_j$需花费$a_{ij}$个单位时间，要求寻找一种零件$J_1, \cdots, J_n$的最优通过顺序$\omega=(i_1, i_2, \cdots, i_n)$使得从第一个零件$J_{i_1}$在$M_1$上开始加工起到最后一个零件$J_{i_n}$在$M_m$上加工完毕止，所历经的总加工时间$T(\omega)$为最短．

当诸零件以$\omega=(i_1, i_2, \cdots, i_n)$的同一次序依次通过诸机床$M_1, M_2, \cdots$时，在加工过程中常常会出现“停工待料”的现象：机床M_k已加工完J_{i_s}，但下一个零件$J_{i_{s+1}}$在M_{k-1}上尚未加工完毕，因而M_k便处于空闲状态直至$J_{i_{s+1}}$在M_{k-1}上加工完毕才能继续工作．对于不同的通过顺序ω，这种停工待料的程度也就不同．“零件加工顺序问题”即为求出一种最佳的顺序ω，使得M_m的累计空闲时间达到最小．

对于两台机床的情形，Johnson 提出了一种行之有效的算法：

在阵$A=(a_{ij})$中找出最小的a_{ij}（若不止一个任取其

一),若 $i=1$, 则将 J_j 排在最前面;若 $i=2$, 则将 J_j 排在最后面. 然后划去该列,继续这一过程,直至全部列都划去即得最优排列.

例如对于表 1 所示的例子,最小元 $a_{22}=2$, $i=2$, 故将 J_2 排在最后. 划去该列后, 最小元为 $a_{11}=a_{24}=3$, 任取其一,例如由 $a_{11}=3$, $i=1$ 即将 J_1 排在最前. 如此反复, 便得最优排列为 $J_1J_3J_5J_4J_2$, 相应的最小加工时间为 $T=28$.

表 1.

	J_1	J_2	J_3	J_4	J_5
M_1	3	7	4	5	7
M_2	6	2	7	3	4

但当 $n\geqslant 3$ 时,情形大为复杂,迄今仍无一个其有效性能与上述 Johnson 法则相比的一般性算法,而且业已证明:的确不存在很"有效"的算法. Ignell 在[88]与 Lomnicki 在[106]中首次将分枝定界算法用于零件加工顺序问题的求解. 其后, 他们的定界方法又有了改进. 为了运用这一算法, 我们首先赋予 $n!$ 个排列以一种树形结构: 根点 O 表示全部的排列, 过 O 点有 n 个分枝 $K_1, K_2, \cdots, K_n$, 分别对应于排列 $\omega=(i_1, i_2, \cdots, i_n)$ 中第一个数 i_1 的 n 种选择方式, 节点 K_s 对应于形如 $\omega=(s, i_2, \cdots, i_n)$ 的排列全体, 过每个节点 K_s, 又引出 $n-1$ 个分枝 $K_{s1}, K_{s2}, \cdots, K_{s,s-1}, K_{s,s+1}, \cdots, K_{sn}$,对应于 $\omega=(s, i_2, \cdots, i_n)$ 中第二个数 i_2 的 $n-1$ 种选择方式,……. 一般若 $D=(s_1, \cdots, s_k)$ 为 $1, 2, \cdots, n$ 的一个 k-排列, 则节点 K_D 表示形如 $(s_1, \cdots, s_k, i_{k+1}, \cdots, i_n)$ 的排列全体. 为了定出诸节点 K_D 上的下界值,我们引述越民义、韩继业在[10]中给出的关于"可行和"这一重要概念的说明.



定义 1. 设零件加工顺序为 $\omega=(i_1,i_2,\cdots,i_n)$，相应的加工时间矩阵为

$$A(\omega)=\begin{bmatrix} a_{1i_1} & a_{1i_2} & \cdots & a_{1i_n} \\ a_{2i_1} & a_{2i_2} & \cdots & a_{2i_n} \\ \cdots & \cdots & \cdots & \\ a_{mi_1} & a_{mi_2} & \cdots & a_{mi_n} \end{bmatrix}.$$

将阵 $A(\omega)$ 中 a_{1i_1} 与 a_{mi_n} 用一条折线相连，此折线只能沿水平方向向右或垂直向下，且仅以 a_{ki_s} 为其顶点. 每一条这样的折线称为对应于 ω 的一可行线. 全体可行线集合即为

$$\begin{aligned}\{l(\omega)\}=\{((1i_1),(1i_2),\cdots,(1,i_{k_1}),\\ (2,i_{k_1}),\cdots,(2,i_{k_2}),\cdots,\\ (m,i_{k_{m-1}}),\cdots,(m,i_{k_m})),\\ 1\leqslant k_1\leqslant k_2\leqslant\cdots\leqslant k_m=n\}.\end{aligned}$$

又称和式 $\sum\limits_{(k,i)\in l(\omega)} a_{ki}$ 为对应于 $l(\omega)$ 的可行和.

下面的重要定理给出了加工时间 $T(\omega)$ 与可行和的关系.

定理 A (越民义、韩继业 [10]). 设诸零件以同一顺序 $\omega=(i_1,\cdots,i_n)$ 依次通过 $M_1,M_2,\cdots,M_m$，则总的加工时间 $T(\omega)$ 等于阵 $A(\omega)$ 中最大的可行和:

$$T(\omega)=\max_{l(\omega)}\sum_{(k,i)\in l(\omega)} a_{ki} \tag{1}$$

由此定理可以引出计算阵 $B=(b_{ij})_{m\times n}$ 最大可行和的递推方法: 以 $T(i,j)$ 记从 b_{11} 到 b_{ij} 的最大可行和，则易见

$$T(i,j)=\max\left(T(i,j-1)+T(i-1,j)\right)+b_{ij}. \tag{2}$$

由(1)式可见，对任意一个可行线 $l(\omega)$，均有

$$T(\omega)\geqslant\sum_{(k,i)\in l(\omega)} a_{ki},$$

亦即每个可行和都给出 $T(\omega)$ 的一个下界. 为了从中选择



一个较好的下界，已提出了若干种方法. 在$m=3$的情形，越民义、韩继业在[10]中提出了一个很好的定界方法. 今结合表2的例子叙述于下. 为书写方便见，我们记 $A=(a_{ij})$ 中，$a_{1j}=a_j$，$a_{2j}=b_j$，$a_{3j}=c_j$.

表 2.

	J_1	J_2	J_3	J_4	J_5	J_6
a_i	6	12	4	3	6	2
b_i	7	2	6	11	8	14
c_i	3	3	8	7	10	12

为了定出节点 K_1 处的下界，首先注意 K_1 对应于形如 $(1, i_2, i_3, \cdots, i_n)$ 的排列全体，故将 J_1 排在最前面，再据 b_i 和 c_i 的值将 J_2 到 J_6 按 Johnson 法则加以重排得到

$$
\begin{array}{c|ccccc}
J_1 & J_2 & J_3 & J_5 & J_6 & J_4 \\
6 & 12 & 4 & 6 & 2 & 3 \\
7 & 2 & 6 & 8 & 14 & 11 \\
3 & 3 & 8 & 10 & 12 & 7
\end{array}
$$

然后计算如下定义的 S_1, S_2 与 S_3，其中 $a=\sum\limits_i a_i$:

$$S_1 = a + \min_{i\neq 1}(b_i + c_i) = 33 + 5 = 38,$$

$$S_2 = a_1 + b_1 + \begin{pmatrix} 2 & 6 & 8 & 14 & 11 \\ 3 & 8 & 10 & 12 & 7 \end{pmatrix}\text{的最大可行和}$$

$$= 13 + 49 = 62,$$

$$S_3 = a_1 + b_1 + c_1 + \sum_{i\neq 1} c_i = 16 + 40 = 56.$$

取 $r_1 = \max(S_1, S_2, S_3) = 62$，由定理A易知

$$\min_{\omega\in K_1} T(\omega) \geqslant \max(S_1, S_2, S_3) = 62.$$

这里用同一文字 K_1 表示形如 $(1, i_2, \cdots, i_n)$ 的排列全体.



用同样方式可算得 $r_2 = 64$, $r_3 = 55$, $r_4 = 59$, $r_5 = 58$, $r_6 = 59$. 按照分枝定界算法的基本思想，我们从中选取下界最小的一个分枝。本例 $r_3 = 55$ 为最小，故选取分枝 K_3，然后进而计算在其后各分枝 $K_{31}, K_{32}, K_{34}, K_{35}, K_{36}$ 上的下界。

设 $D = (s_1, \cdots, s_k)$ 是 $1, 2, \cdots, n$ 的一个 k-排列，确定在结点 K_D 处下界的一般方法为：首先根据 b_j 和 c_j 的值将诸零件 $J_p (p \neq s_j, j = 1, \cdots, k)$ 按 Johnson 法则重排成 $(s_{k+1}, \cdots, s_n)$，然后令

$$S_1 = a + \min_{i \in \{s_{k+1}, \cdots, s_n\}} (b_i + c_i),$$

$$S_2 = \text{阵} \begin{pmatrix} a_{s_1}, & \cdots, & a_{s_k} \\ b_{s_1}, & \cdots, & b_{s_k} \end{pmatrix} \text{的最大可行和}$$

$$+ \text{阵} \begin{pmatrix} b_{s_{k+1}}, & \cdots, & b_{s_n} \\ c_{s_{k+1}}, & \cdots, & c_{s_n} \end{pmatrix} \text{的最大可行和},$$

$$S_3 = \text{阵} \begin{bmatrix} a_{s_1} \cdots a_{s_k} \\ b_{s_1} \cdots b_{s_k} \\ c_{s_1} \cdots c_{s_k} \end{bmatrix} \text{的最大可行和}$$

$$+ \sum_{i=k+1}^{n} c_{s_i},$$

并取 $r_D = \max(S_1, S_2, S_3)$，由定理 A 易知

$$\min_{\omega \in K(D)} T(\omega) \geqslant r_D,$$

故可取 r_D 为节点 K_D 处的下界。

在本例中 $r_{31} = 60$, $r_{32} = 62$, $r_{34} = 60$, $r_{35} = 56$, $r_{36} = 59$. 其中以 $r_{35} = 56$ 为最小，故沿分枝 K_{35} 继续前进。然后按上述方法算得节点 $K_{351}, \cdots, K_{356}$ 处的下界 $r_{351} = 60$, $r_{352} = 60$, $r_{354} = 60$, $r_{356} = 57$. 因 r_{356} 最小，故继续算出 $r_{3561} = 59$, $r_{3562} = 57$, $r_{3564} = 57$. 此时，$r_{3562} = r_{3564}$ 同取最小值，任取其一，例如取定节点 K_{3562}. 过 K_{3562} 只有两个分



枝，分别对应于排列 $\omega_1=(356214)$ 与 $\omega_2=(356241)$，直接计算得出 $T(\omega_1)=59$，$T(\omega_2)=57$。至此已抵达叶点 K_{ω_2}，将该点的 $T(\omega_2)$ 值与行进过程中诸节点 K_D 处计得的下界相比，我们发现，诸下界均 $\geqslant 57$。因沿下界 $\geqslant 57$ 的分枝前进决不会得比 57 更小的 $T(\omega)$ 值，故 $T(\omega_2)=T(356241)$ 便为最优加工时间。(此例中若沿 K_{3564} 前进，仍得出另外二种最优排列：$T(356412)=T(356421)=57$。)全部计算过程如图 4 所示。

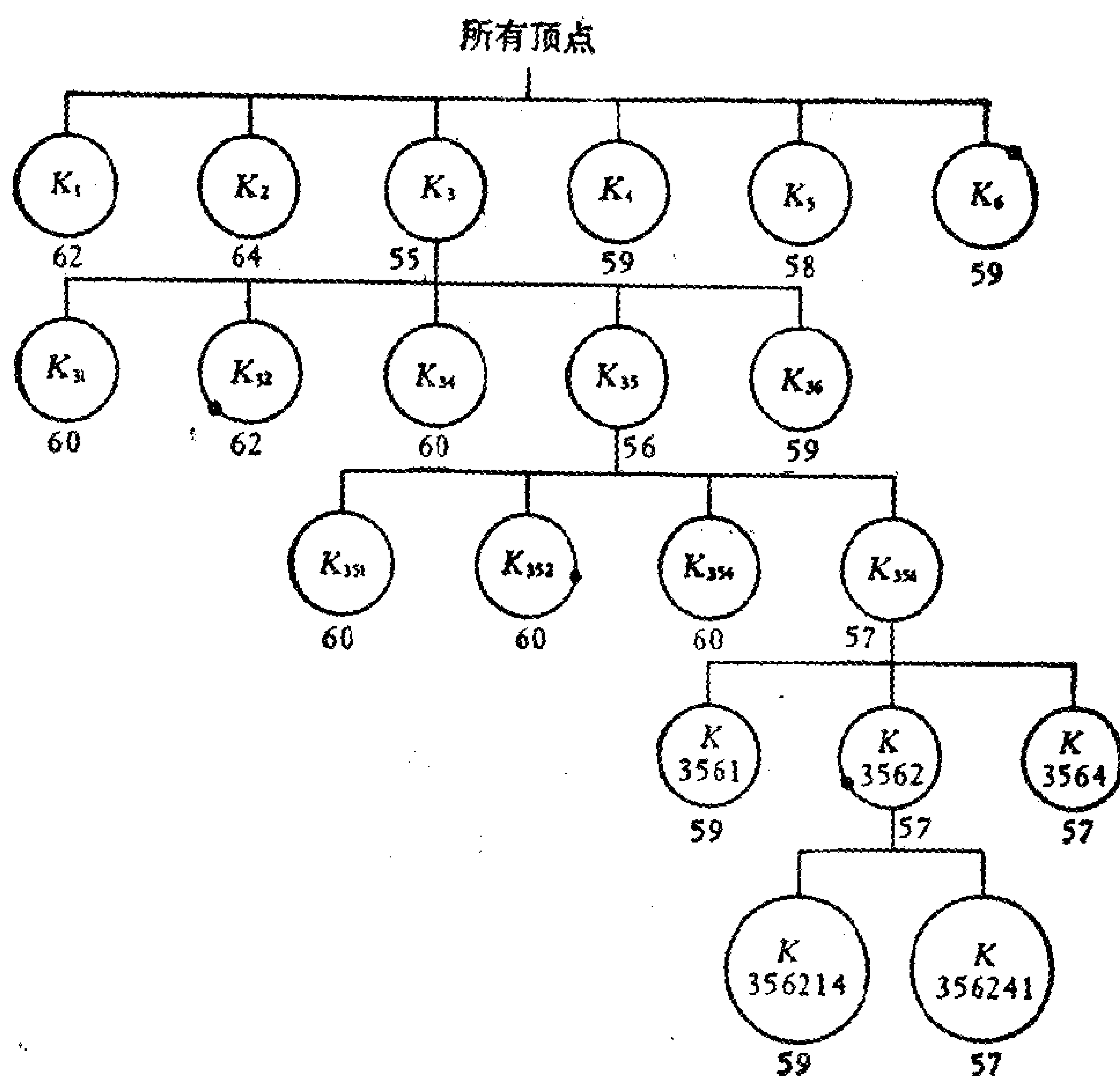


图 4. 用分枝定界法求解零件加工顺序问题的树形图

在一般情形，当我们每次沿下界最小的一枝到达叶点 K_ω 后，若发现计得的 $T(\omega)$ 值比在行进过程中计得的某一节点 K_D 处的下界 r_D 为大，则表明沿 K_D 前进有可能找到比



$T(\omega)$ 更小的加工时间。故此时尚须回过头来，从 r_D 值最小的节点 K_D 开始重复上述计算过程，直至最后到达某个叶点，相应的 $T(\omega)$ 均不超过各节点 K_D 处的下界为止。

图 5 给出了这一算法的计算框图，框图中 K_D，r_D 的定义见前所述，即当 $D=(s_1, \cdots, s_k)$ 时，K_D 表示形如 $(s_1, \cdots, s_k, i_{k+1}, \cdots, i_n)$ 的排列全体。D^* 表示在算法行进过程中已确定的部分排列，又 $S=\{1, 2, \cdots, n\}$。此外，当 $D^*=(s_1, \cdots, s_k)$ 时，记 $S\backslash D^*=\{i | i\in S, i \neq s_1, s_2, \cdots, s_k\}$。又以 z^* 记最优顺序的加工时间的上界，即 $z^* \geqslant \min\limits_{\omega} T(\omega)$。

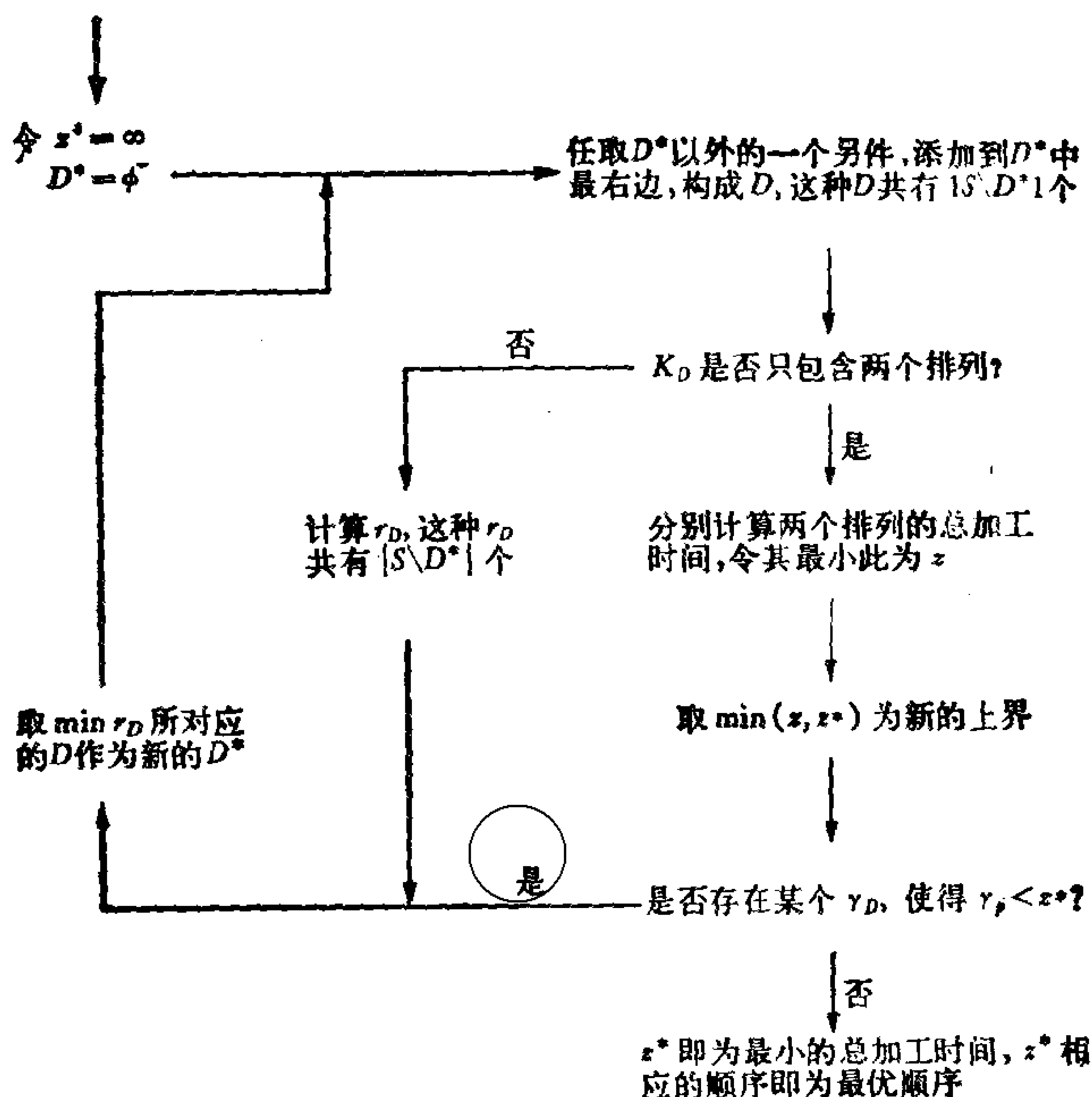


图 5. 用分枝定界算法解零件加工顺序问题的框图

ϕ表示空集



在算法的进行过程中，我们还需要在给出阵 $B=(b_{ij})$ 及排列 $\omega=(s_1, s_2, \cdots, s_n)$ 后求出阵

$$B(\omega)=(b_{is_j})$$

的最大可行和. 此部分程序可写成子程序的形式,在转子前,主程序应形成完阵 $B=(b_{ij})$ 及排列 $\omega=(s_1, \cdots, s_n)$.

基于递推式(2),用初级会话语言 *BASIC* 可以写出该子程序如下. 程序中利用关系式

$$\max(x, y)=(|x+y|+|x-y|)/2,$$

尤当 $x, y \geqslant 0$ 时,式中 $|x+y|$ 可代之以 $x+y$. 又程序中将所得的诸 $T(i, j)$ (即从 b_{1s_1} 到 b_{is_j} 的最大可行和)组成阵 $C=(T(i, j))$, $T(m, n)$ 即为所求的最大可行和 $T(\omega)$, 在返回主程序时,将此值赋予变元 T.

(主程序已有 *DIM C(M, N)*)

```
500 REM SUBROUTINE
502 FOR J = 1 TO N
504       LET C(0, J) = 0
506 NEXT J
508 FOR I = 1 TO M
510       LET C(I, 0) = 0
512 NEXT I
514 LET S(0) = 0

516 FOR I = 1 TO M
518       FOR K = 1 TO N
520             LET J = S(K)
522             LET H = S(K - 1)
524             LET X = C(I - 1, J)
526             LET Y = C(I, H)
```




```
528          LET C(I, J) = (X + Y + ABS(X
                              - Y))/2 + B(I, J)

530     NEXT K
532 NEXT I
534 LET T = C(M, N)
536 RETURN
```

注. 由于阵的第零行,零列之值 0 及 $S(0)=0$,在计算过程中一经形成,不再改变,故语句 502～514 实际上可移到主程序一开始置初值部分中,不必每次转子时重复形成.

本节例 2 中的 a_i, b_i 及 c_i 之值(表 2)取自 Lomnicki [106],但定界方法采用越民义、韩继业[10]中者.由于这种定界方法是迄今较佳的一种,因此上面的计算比 Lomnicki [106] 中所列出的大为减少. 第一次抵达的叶点便是最小值点.

最后仍需指出的是,尽管顺路返回算法与分枝定界算法在遍数的技巧上作了相当大的改进,但这两种算法所需的工作量依然是很大的. 对各类问题,我们仍需结合问题的特点,努力寻求有效的算法. 对于优化问题,我们还应深入研讨最优解的结构,以便在遍数过程中,预先排除更多的分枝,减少计算量. 例如越民义、韩继业在[9]中曾得出了最优加工顺序中,确定相邻两零件先后次序的充分条件,较 Nabeshima [115] 中的同类条件简化很多. 对于三台机床的情形,在某些极为特殊的场合,可以较快地得出最优顺序,但在一般情形,尚有待于更深入的研讨.



6.2. 计算机算法分析：分类问题的“气泡”算法

本节将综合运用前面各章中介绍的组合计数方法于计算机算法分析的一个例子：分类问题的“气泡”算法.

现代电子计算机的应用范围早已从传统的数值问题的求解扩大到诸如生产过程控制，大规模数据处理等一系列领域中，新的问题和算法不断出现．如何寻求一个可行的算法，如何从数学上分析某种算法的有效性，又如何比较为了达到同一目标而提出的各不同算法的优劣，构成了计算机算法分析这一引人入胜的新课题．评价一个算法的优劣标准有很多，例如 (i) 求解结果的精度；(ii) 运算时间的长短；(iii) 占用存储单元的多少以及 (iv) 程序的长度和复杂性等等． 其中 (iii) 的估计一般较为容易，(iv) 又多少和各个机器的特点有关，而对于非数值问题，不同的算法常常能得到同一结果，因此对于此种算法，运算次数的分析尤见重要． 本节将以分类问题的“气泡”算法为例，着重说明组合计数方法的应用．

所谓分类问题，简单地说，就是将 n 个位置上的 n 个“数”，按某种规定的顺序重新排列． 用计算机操作系统中常用的术语来叙述就是：给出一个由 n 项“记录”$R_1, \cdots, R_n$ 组成的一个文件，每个记录 R_i 附有一个“主题词”K_i，假设诸 K_i 可以相互比较(亦即诸 K_i 构成一个线性序集，见 3.3 节)．分类问题归结为求出 $1, 2, \cdots, n$ 的一个排列 $\sigma(1), \cdots, \sigma(n)$，使得 $K_{\sigma(1)} \leqslant K_{\sigma(2)} \leqslant \cdots \leqslant K_{\sigma(n)}$． 作为 K_i 的例子如符号语言程序中各段的标号，它们一般由 26 个拉丁字母和数字 0～9 组成． 在程序编译时，第一次扫描一般需将程序中出现的诸标号按字典次序排列成表． 分类问题在计算机数据处理、编译程序、操作系统等软件系统中有着重要的应用．Knuth



在[98] V.3 中甚至引用一家厂商的统计断言：当今计算机约有四分之一的运行时间花费在运算对象的“分类”上.

下面为叙述简单见，我们仍将 n 个“主题词” K_i 设想成 n 个数 $1, 2, \cdots, n$. 迄今已有不少分类问题的算法，如在 Knuth [98]V.3 中就列举了约 25 种不同的算法，其中之一“气泡”算法的基本思想如下：设初始排列为 $P=(a_1, a_2, \cdots, a_n)$，我们首先比较 a_1 与 a_2，若 $a_1 \leqslant a_2$，则不作变动，即令 $a_1' = a_1$，$a_2' = a_2$；若 $a_1 > a_2$，则交换两者的位置，令 $a_1' = a_2$，$a_2' = a_1$. 接着比较 a_2' 与 a_3，a_3' 与 a_4，$\cdots$，a_{n-1}' 与 a_n. 经过这一次扫视得到排列 $P' = (a_1', a_2', \cdots, a_n')$. 对 P' 再重复这一过程，如此反复，直至最后得到 $P^{(k)} = (a_1^{(k)}, \cdots, a_n^{(k)})$ 满足 $a_1^{(k)} \leqslant \cdots \leqslant a_n^{(k)}$ 为止. 表 1 给出了当初始排列 $P_1 = (4162735)$ 时，逐次扫描的结果.

在这一算法的进行过程中，大的元宛如水中的“大气泡”一般逐渐上升，直至顶住比它更大的“气泡”为止，故形象地名为“气泡”算法. 从表 1 所示例子可见，每次扫视中最后一个上升的“气泡”(如 P_3 中的“6”)在下一次扫视中便不再上升. 因此若在 P_k 中 $d+1$ 为最后一个上升的“气泡”所到达的位置，则在下一次扫视中，只需扫视前面 d 个元 $a_1^{(k)}, \cdots, a_d^{(k)}$.

表 1. “气泡”算法例

P_1	P_2	P_3	P_4	P_5
5	7	7	7	7
3	5	6	6	6
7	3	5	5	5
2	6	3	4	4
6	2	4	3	3
1	4	2	2	2
4	1	1	1	1



由此引出“气泡”算法的形式描述如下，其中工作单元 d 用来存放上述的 d 值，亦即每次扫描开始时需要确定其最后位置的元 $a_i^{(k)}$ 的最大下标 i；而工作单元 t 则指出正在交换的一对元（a_j 与 a_{j+1}）。每次扫视开始时初值为 0。

“气泡”算法.

1.（置 d 的初值）$n \to d$.

2.（循环）$0 \to t$； 对于 $j=1, 2, \cdots, d-1$，完成第 3 步中所示的运算.

3.（比较与交换）若 $a_j > a_{j+1}$，则交换 a_j 与 a_{j+1} 的位置，并将 j 值送入 t: $j \to t$.

4.（结束否?）若 $t=0$，算法结束，否则 $t \to d$，去步 2.

这一算法的运算次数涉及到三类量： 1. 扫视的次数 a; 2. 交换的次数 b; 3. 比较的次数 c. 今逐一分析如下.

显然，“气泡”算法的运算次数与初始排列 $P=(a_1, a_2, \cdots, a_n)$ 中反序的多少有关. 此处所谓 (a_i, a_j) 构成一对反序，系指 $i<j$，但 $a_i > a_j$. 例如 $P=(4162735)$ 中，有 $(4,1), (4,2), \cdots, (7,5)$ 等共 8 对反序. 今以 b_i 记排列 P 中位于“i”左边且大于 i 的元数，并称 $B=(b_1, b_2, \cdots, b_n)$ 为排列 P 的反序表. 例如对表 1 中的 P

$$P=(4162735),$$
$$B=(1230200),$$

此因在 P 中位于“3”左边的 4, 1, 6, 2, 7 中有 3 个数 4, 6, 7 大于 3，故 $b_3=3$；位于 6 左边的 1, 4 均小于 6，故 $b_6=0$ 等等. 由定义可见，$0 \leqslant b_j \leqslant n-j$. 不难证明任一 $B=(b_1, b_2, \cdots, b_n)$ 只要满足

$$0 \leqslant b_j \leqslant n-j \quad (j=1, 2, \cdots, n), \qquad (1)$$

总可以找到唯一的一个排列 P，使它的反序表为 B. 例如对上例所示的 $B=(1230200)$，因 $b_6=0$，故 $P=(\cdots 6 \cdots$



$7\cdots)$，再由 $b_5=2$，可见 $P=(\cdots6\cdots7\cdots5\cdots)$，复由 $b_4=0$ 可见 $P=(\cdots4\cdots6\cdots7\cdots5\cdots)$，如此反复便可得到 $P=(4162735)$。因此反序表B中诸 b_j 的选取是独立的，只须满足 (1) 即可。显然 $b=\sum b_i$ 给出了排列P的全部反序个数。

下面我们假设气泡算法开始执行时，初始排列 $P_1=(a_1, a_2, \cdots, a_n)$ 的反序表为 $(b_1, b_2, \cdots, b_n)$。在气泡算法中，初始排列每有一组反序，就需进行一次交换，因而总的交换次数 b 等于P的所有反序个数

$$b=b_1+b_2+\cdots+b_n. \tag{2}$$

其次，试考察气泡算法历次扫视后所得的排列，并算出相应的反序表

$$P_1=4162735,\quad B_1=1230200,$$
$$P_2=2531647,\quad B_2=0120100,$$
$$P_3=2315467,\quad B_3=0010000.$$

我们发现，若记 $B_k=(b_1^{(k)}, \cdots, b_n^{(k)})$，则在第$k$次扫视后，$B_k$ 中的正元都减 1，即

$$b_i^{(k+1)}=(b_i^{(k)}-1)_+, \tag{3}$$

其中 $(x)_+$ 定义为

$$(x)_+=\begin{cases}x, & x\geqslant 0;\\ 0, & x<0.\end{cases} \tag{4}$$

(3)式的证明甚易，此处从略，读者可作为一个练习。由(3)式可见，“气泡”算法共需进行

$$a=1+\max(b_1, b_2, \cdots, b_n) \tag{5}$$

次扫视。在每次扫视中共进行了 $d-1$ 次比较，故共需

$$c=c_1+c_2+\cdots+c_a \tag{6}$$

次比较，其中 c_j 等于从排列 P_j 得到 P_{j+1} 所需的比较次数。今证



$$c_j = \max\{b_i + i \mid b_i \geqslant j-1\} - j. \tag{7}$$

实际上，假设经过了 $j-2$ 次扫视后得到 $P_{j-1}=(a'_1,\cdots,a'_n)$，其反序表 $B_{j-1}=(b'_1,\cdots,b'_n)$。于是 $b'_i=(b_i-j+2)_+$，$b'_i>0$ 当且仅当 $b_i\geqslant j-1$。假定在 P_{j-1} 中第 l 个位置上的元 $a'_l=i$，又设在 a'_l 的左边有 b_L 个元 $>i$，S_L 个元 $<i$；而在 a'_l 的右边有 b_R 个元 $>i$，S_R 个元 $<i$，则由定义 $b_L=b'_i$，$S_L+S_R=i-1$，$b_L+S_L=l-1$，由此可得 $S_R=b'_i-i+l$，亦即在 a'_l 的右边还有 b'_i+i-l 个元比 i 小。因此若 $b'_i>0$，则 a'_l 左边的最大元至少向右移动到位置 $l+S_R=b'_i+i$ 处。但若 s 为 P_{j-1} 中最右边一个需要改变位置的元，则 $b'_s>0$。由此可见，经第 $j-1$ 次扫视后最后一个“气泡”应上升到 b'_s+s 位置上。于是第 j 次扫视时，共需进行 b'_s+s-2 次比较，此即 $c_j=b'_s+s-2=(b_s-j+2)+s-2=b_s+s-j$。

这样我们就得到了“气泡”算法中三类运算次数的表示式 (2)，(5)与 (6)。为了求得气泡算法的平均运算次数，我们必须分别求出 a, b, c 三个量关于全部 $n!$ 个排列的平均值，并定出它们的渐近值。这构成了一个相当复杂的组合计数问题。

我们首先来求出交换次数 b 的平均值 $\bar{b}=V/n!$，V 为 $n!$ 个排列的全部反序个数。如前，记 $n!$ 个排列全体构成的集合为 S_n。若以 $I_n(k)$ 表示 S_n 中恰有 k 个反序的排列个数，则由排列与反序表间的一一对应关系，可见 $I_n(k)$ 等于不定方程

$$b_1+b_2+\cdots+b_n=k,$$
$$0\leqslant b_i\leqslant n-i \qquad (i=1,2,\cdots,n)$$

的解的个数。由此易见，$I_n(k)$ 的生成函数为

$$G_n(x)=I_n(0)+I_n(1)x+I_n(2)x^2+\cdots$$



$$= 1 \cdot (1 + x)(1 + x + x^2) \cdots (1 + x + \cdots + x^{n-1}).$$

一个随机选取的排列恰有 k 的反序的几率为 $p_n(k) = I_n(k)/n!$，故 $p_n(k)$ 的生成函数 $P_n(x) = \sum p_n(k) x^k = G_n(x)/n! = h_1(x) h_2(x) \cdots h_n(x)$，其中

$$h_k(x) = (1 + x + \cdots + x^{k-1})/k.$$

因此，对于随机选取的排列，其反序的平均个数等于

$$\begin{aligned} b &= \sum k p_n(k) = ((d/dx) P_n(x))_{x=1} \\ &= \sum_{k=1}^{n} (h_1 h_2 \cdots (dh_k/dx) \cdots h_n)_{x=1} \\ &= \sum_{k=1}^{n} ((d/dx) h_k)_{x=1} \\ &= \sum_{k=1}^{n} (1 + 2 + \cdots + (k-1))/k \\ &= \sum_{k=1}^{n} (k-1)/2 = n(n-1)/4. \end{aligned}$$

此即气泡算法的平均交换次数为

$$\bar{b} = (n^2 - n)/4. \tag{8}$$

其次我们计算扫视次数 a 的平均值 $\bar{a}$. 由(5)式，欲 $a \leqslant k$ 当且仅当 $b_i \leqslant k - 1$ $(i = 1, \cdots, n)$，另一方面又必须有 $0 \leqslant b_i \leqslant n - i$. 因此若 $n - i > k - 1$ 或 $i \leqslant n - k$，则 b_i 有 k 种选法（即 $0, 1, \cdots, k-1$）；而当 $n - i \leqslant k - 1$ 或 $i \geqslant n - k + 1$ 时 b_i 有 $(n - i + 1)$ 种取法，故满足 $a \leqslant k$ 的反序表共有 $k^{n-k} k!$ 个. 由此可见满足 $a = k$ 的反序表个数共有 $k^{n-k} k! - (k-1)^{n-k+1} (k-1)!$ 个. 于是 $a = k$ 的几率 $p_k = (k^{n-k} k! - (k-1)^{n-k+1} (k-1)!)/n!$. 应用分部求和公式(4.2.15)可见 p_k 的平均值为



$$\sum_{k=1}^{n} kp_k = \sum_{k=1}^{n} k((k^{n-k}k!/n!)$$
$$- ((k-1)^{n-k+1}(k-1)!/n!))$$
$$= (n+1) - \sum_{k=1}^{n} k^{n-k}k!/n!$$
$$= (n+1) - P(n).$$

其中 $P(n) = \sum_{k=1}^{n} k^{n-k}k!/n!$，由 4.2 节例 2 所得 $P(n) \sim \sqrt{\pi n/2}$，因此气泡算法的平均扫视次数为

$$\bar{a} = n - \sqrt{\pi n/2} + O(1). \tag{9}$$

最后我们分析比较次数 c。由(7)式知 $c_j \leqslant k$ 当且仅当 (i) $b_i \leqslant n-i$; (ii) 不等式 $b_i + i \leqslant k + j$ 或 $b_i < j - 1$ 之一成立。此处注意：在第 j 次扫视开始时，比较的次数 c_j 至多为 $n-j$，因此可设 $k \leqslant n-j$。为了计算满足上述条件 (i) 与 (ii) 的反序表 $\{b_i\}$ 的个数 N_{jk}，我们记 $Z_l = \{0, 1, \cdots, l\}$，$S_1 = Z_{j-2}$，$S_2 = Z_{k+j-i}$，$S_3 = Z_{n-i}$，则易见

$$N_{jk} = |(S_1 \cap S_3) \cup (S_2 \cap S_3)|.$$

由(3.4.9)式

$$N_{jk} = |S_1 \cap S_3| + |S_2 \cap S_3| - |S_1 \cap S_2 \cap S_3|.$$

今显然

$$|S_1 \cap S_3| = (\min(j-2, n-i) + 1)_+,$$
$$|S_2 \cap S_3| = (\min(k+j-i, n-i) + 1)_+,$$
$$|S_1 \cap S_2 \cap S_3| = (\min(j-2, k+j-i,$$
$$n-i) + 1)_+.$$

当 $i \geqslant n-j+2$ 时，$j-2 \geqslant n-i$，于是 $|S_1 \cap S_2 \cap S_3| = |S_2 \cap S_3|$，故 $N_{jk} = |S_1 \cap S_3| = n-i+1$；而当 $k+2 \leqslant i < n-j+2$ 时 $k+j-i \leqslant j-2$，同理可得 $N_{jk} = |S_1 \cap$



$S_3| = j-1$;最后当 $i < k+2$ 时, $k+j-i > j-2$,注意 $k+j \leqslant n$, 同样有 $N_{jk} = |S_2 \cap S_3| = k+j-i+1$. 综合所得可见满足 $c_j \leqslant k$ 的反序表 $B = \{b_i\}$ 共有 $\prod\limits_{i \geqslant (n-j+2)} (n-i+1) \prod\limits_{n-j+2 > i \geqslant k+2} (j-1) \prod\limits_{k+2 > i} (k+j-i+1) = (j+k)!(j-1)^{n-j-k}$ 种取法. 记 $f_j(k) = (j+k)!(j-1)^{n-1-k}$, 应用分部求和公式(4.2.15),可见 c_j 的平均值为

$$\bar{c}_j = \sum_{k=0}^{n-j} k(f_j(k) - f_j(k-1))/n!$$

$$= \left((n+j+1)f_j(n-j) - \sum_{k=0}^{n-j} f_j(k)\right)/n!$$

$$= (n-j+1) - \sum_{k=0}^{n-j} f_j(k)/n!,$$

因此 c 的平均值

$$\bar{c} = \sum_{j=1}^{n}(n-j+1) - \sum_{j=1}^{n}\sum_{k=0}^{n-j} f_j(k)/n!,$$

代入 $f_j(k)$ 的表示式,并作变量代换 $s = j+k$, $r = j-1$, $m = n+1$, 即得

$$\bar{c} = \binom{n+1}{2} - \sum_{0 \leqslant r < s \leqslant n} s!\, r^{n-s}/n!$$

$$= \binom{m}{2} - W_m,$$

其中

$$W_m = (1/(m-1)!) \sum_{1 \leqslant t < m} (m-t)! \times \sum_{0 \leqslant r < m-t} r^{t-1}.$$



由命题(2.5.8)，

$$\sum_{0\leqslant r<N} r^{t-1} = (N^t/t) - (1/2)N^{t-1} + \cdots$$

$$= (1/t)\sum_{j\geqslant 0}\binom{t}{j} B_j(N^{t-j} - \delta_{tj}), \qquad (10)$$

其中第一项

$$(N^t/t)_{N=(m-t)} = (m-t)^t/t$$

对

$$(W_m)/m = \frac{1}{m!}\sum_{1\leqslant t<m}(m-t)!\sum_{0\leqslant r<m-t} r^{t-1}$$

的贡献为

$$(1/m!)\sum_{1\leqslant t<m}(m-t)!(m-t)^t t^{-1}.$$

由 4.2 节例 3 知上一和式等于 $(\log m + \gamma + \log 2)/2 + O(m^{-1/2})$. (10) 中其余诸项的一般形式为 $t^q N^{t-p}$ $(q \leqslant p-1, p \geqslant 1)$ 或 $O(1)\delta_{tp}$，在这些项中（按绝对值）最大的贡献来自 N^{t-1}. 即来自和式

$$(1/m!)\sum_{1\leqslant t<m}(m-t)!(m-t)^{t-1}.$$

但易证

$$\sum_{1\leqslant t<m}(m-t)!(m-t)^{t-1}/m!$$

$$\sim (1/m)\sum_{1\leqslant t<m}(m-t)!(m-t)^t$$

$$\sim (1/m)\sqrt{m\pi/2} = O(m^{-1/2})$$

(见 4.2 节例 2). 因此(10)中其余诸项对 $(1/m)W_m$ 的贡献为 $O(m^{-1/2})$. 由此可见

$$(W_m/m) = (\log m + \gamma + \log 2)/2 + O(m^{-1/2}),$$

或



$$W_m = (m\log m)/2 + (\gamma + \log 2)m/2 + O(m^{1/2}),$$

此即平均比较次数

$$\bar{c} = \binom{n+1}{2} - (n\log n)/2 - (\gamma + \log 2)m/2 + O(m^{1/2})$$
$$= (n^2 - n\log n - (\gamma + \log 2 - 1)n)/2 + O(n^{1/2}). \tag{11}$$

至此，"气泡"算法中所涉及的三类运算次数的表示式及其渐近值已全部得出. 因此若在某一特定计算机中，交换两个元，比较两元大小及扫视部分程序段执行时间已知后，立即可算出"气泡"算法的平均执行时间. 对分类问题的其他算法分析结果表明，"气泡"算法并不是很好的算法，它的缺点在于初始排列的每一对反序都导致一次交换，这一点是可以避免的. 关于分类问题的其他算法可见 Knuth[98] V.3, Nivat [120] 等.

关于计算机算法的设计和分析已有不少工作，如 Aho [18], Even [60], Meersman [111], Nijenhuis [118], Yeh [163] 等.



参 考 文 献

[1] 万哲先、戴宗铎、冯绪宁、阳本傅，有限几何与不完全区组设计的一些研究，科学出版社，1966.

[2] 万哲先，代数和编码，科学出版社，1976.

[3] 王竹溪，统计物理学导论，高教出版社，1956.

[4] 华罗庚，从杨辉三角谈起，中国青年出版社，1962.

[5] 华罗庚、王元，数值积分及其应用，科学出版社，1963.

[6] 闵嗣鹤、严士健，初等数论，高教出版社，1957.

[7] 唐有祺，统计力学及其在物理化学中的应用，科学出版社，1974.

[8] 徐利治，数学分析的方法及例题选讲，商务出版社，1955.

[9] 越民义、韩继业，n 个零件在 m 台机床上的加工顺序问题 (I)，中国科学，**5**(1975)，462—470.

[10] 越民义、韩继业，排序问题中的一些数学问题，数学的实践和认识，1976，3，59—70；4，62—77.

[11] 傅钟孙，A problem on non-sensed circular permutations，国立武汉大学理科季刊，八卷，1.1—1.15，1942.

[12] 蒲吉，关于 0.618 的由来及其最优性，数学的实践与认识，1972，7，3—17.

[13] 屠规彰，关于组合数论的一个猜测，自然杂志，**1**(1978)，274.

[14] 屠规彰，关于最优搜索树的一个不等式，科学通报(外文版)，**25**(1980)，713—715.

[15] 屠规彰，GF(2) 上一类三次形的典式，数学学报，**28**(1980)，1，13—14.

[16] 屠规彰，三阶 Reed-Muller 码中一类码字的计数，数学学报，28(1980)，1，13—24.

[17] 屠规彰，三项齐次递推式的一般解公式(尚未发表)。

[18] Aho, A. V. et al., The design and analysis of computer algorithms, Addison-Weley, 1974.

[19] Aigner, M., Kombinatorik, 1. Grundlagen und Zähltheorie, Springer-Verlag, 1975.

[20] Akers, S. B. Jr., Fault diagnosis as a graph coloring problem, *IEEE Trans. Comput.*, **23**(1974), 706—713.

[21] Albree, J., The gcd of certain binomial coefficients, *Math. Mag.*, **45**(1972), 259—261.

[22] Alter. R., Some remarks and results on Catalan numbers. in "Proc. 2nd Louisiana Conf. on combinatorics, graph theory and computing." ed. by R. C. Mullin et al., 109—132, 1971.

[23] Andrews, G. E., On the foundations of combinatorial theory V. Eulerian differential operators, *Stud. Appl. Math.*, **50**(1971),



345—375.

[24] Appel, K., The proof of the Four-Color problem. *New Sci.*, 72 (1976), 154—155.

[25] Appel, K. and Haken, W., Every planer map is four colorable, *Bull. Amer. Math. Soc.*, **82**(1976), 711—712.

[26] Азагян, А. А. и Тамразян, Р. А., Об одном методе перестановок из *n* различных символов, *ДАН АрмССР*, **61**(1975), 262—268.

[27] Balaban, A. T. and Harary, F.. Chemical graphs IV, Dihedral groups and monocylic acromatic compounds, *Rev. Roumaine. Chim.*, **12**(1967), 1511—1515.

[28] Bammel, S. E. and Rothstein, J.. The number of 9×9 Latin squares, *Discrete Math.*, **11**(1975), 93—95.

[29] Baumert, L. D. and McEliece, R. J. Weights of irreducible cylic codes, *Inform. & Control*, **20**(1972). 158—175.

[30] Beckenbach, E. F. et al., (ed.) Applied combinatorial mathematics, Wiley, 1964.

[31] Bender, E. A., A generalized q-binomiál Vandermonde convolution, *Discrete Math.*, **1**(1971), 115—119.

[32] ——————, Central and local limit theorems applied to asymptotic enumeration, *J. C. T.*, A**15**(1973). 91—111.

[33] ——————, Asymptotic methods in enumeration, *SIAM Rev.*, **16**(1974). 485—515.

[34] Bender, E. A. and Goldman, J. R. Enumerative uses of generating functions. *Indiana Univ. Math.*, **20**(1971), 753—765.

[35] ——————, Möbius inversion in combinatorial analysis, *Amer. Math. Month.*, **82**(1975), 789—802.

[36] Berge, C., Pricipes de combinatoire, Dunod. 1968.

[37] Berlekamp, E. R., Algebraic coding theory, McGraw-Hill, 1968.

[38] Berlekamp. E. R. et al., Gleason's theorem on self-dual codes. *IEEE Trans. Inform. Theory* **18**(1972), 409—419.

[39] Bregman, L. M., Some properties of nonnegative matrices and of their permanents, *Dokl. Akad. Nauk. SSSR*, **211**(1973), 27—30.

[40] Brualdi, R. A. and Gibson, P. M., Convex polyhedra of doubly stochastic matrices, 1. Applications of the permanent function. *J. C. T.*, A**22**(1977), 194—230.

[41] de Bruijn, N. G., Asymptotic methods in analysis, North-Holland, 1958.

[42] ——————, Generalization of Pólya's foundamental theorem in enumerative combinatorial analysis, *Kon. Ned. Akad. Weten-*



sch. Ser. **A62**(1959), 56—79.

[43] ——————, Pólya's theory of counting, in [30] 144—184, 1964.

[44] ——————, A survey of generalization of Pólya's enumeration theorem. *Nieuw Arch. Wisk.*, **19**(1971), 89—112.

[45] ——————, Enumeration of mapping patterns, *J. C. T.*, A **12**(1972), 14—20.

[46] Cadgan, C., Time-tabling scheduling and the colouring of graphs, *N. Z. Math. Mag.*, **11**(1974), 1—3.

[47] Calitz, L., Generating functions, *Fibonacci Quart.*, **7**(1969), 359—393.

[48] ——————, Permutations with prescribed pattern, *Math. Nachr.*, **58**(1973), 31—53.

[49] ——————, Permutations and sequences, *Adv. Math.*, **14** (1974), 92—120.

[50] ——————, Permutations, sequences and special functions, *SIAM Rev.*, **17**(1975), 298—322.

[51] Comtet, L., Advanced combinatorics, The art of finite and infinite expansions, Dordrecht, Reidel. 1974.

[52] Comete, L. and Fiolet, M., Sur le mode des nombres de Stirling de seconde espece, *C. R. Acad. Sci.*, Paris, ser. A—B, 180(1975), A1263—A1265.

[53] Crapo, H. H., Möbius inversion in a lattice, *Arch. Math.*, **19** (1968), 595—607.

[54] Сидельников, В. М., О спектре весов двоичных кодов Боуза-Чоудхури-Хоквинлема, *Проблемы передачи информации*, **7** (1971), 14—22.

[55] Dénes, J. and Keedwell, A. D., Latin square and their applications, Akadémiai Kiadó, 1974.

[56] Dickson, L. E., Linear groups, Dover, 1958.

[57] Doubilet, P. et al., On the foundations of combinatorial theory VI, The idea of generating function, in "6th Berkeley symp. on math. stat. and prob.", Univ. Calif. Pr., 1971.

[58] Erdös, P. and Kaplansky, I., The asymptotic number of Latin rectangles, *Amer. J. Math.*, **68**(1946), 230—236.

[59] Erdös, P., The art of counting, MIT Pr., 1973.

[60] Even, S., Algorithmic combinatorics, Macmillan, 1973.

[61] Everett, C. J. and Stein, P. R., The asymptotic number of integer stochastic matrices, *Discrete Math.*, **1**(1971), 55—72.

[62] Feinstein, A., Foundations of information theory, McGraw-



Hill, 1958.(中译本：A. 范恩斯坦,信息论基础,科学出版社,1964.)
[63] Feller, W., An introduction to probability theory, Vol. I, 3rd ed., John Wiley, 1968.
[64] Фихтенгольц, Г. М., Курс дифференциального и интегрального исчсление, Т. I—III, Гостехиздат 1948 (中译本：Г. М. 菲赫钦戈里茨,微积分学教程,高教出版社.)
[65] Foata, D., La génératrice exponentielle dans les problèmes d'enumération, Presses Univ., Montreal, 1974.
[66] Garey, M. R., An application of graph colouring to printed circuit testing, in "16th Annu. symp. found. comput. sci.", 178—183, 1975.
[67] Goldman, J. and Rota, G. C., The number of subspaces of a vector space, in "Recent progress in combinatorics" ed. by W. T. Tutte, 75—83, 1969.
[68] ——————, On the foundations of combinatorial theory IV: Finite vector spaces and Eulerian generating functions, *Stud. Appl. Math.*, **49**(1970), 239—258.
[69] Golomb, S. and Baumert, L., Backtrack programming. *J. Assoc. Comp. Mach.*, **12**(1965). 516—524.
[70] Good, I. J., Generalization to several variables of Lagrange's expansion, *Proc. Camb. Phil., S.*, **56**(1960), 367—380.
[71] Gordon, M., Combinatorial short-cuts to statistical weight and enumeration of chemical isomers, in [116], 231—238, 1976.
[72] Gould, H. W., Combinatorial identities, Morgantown printing Co.. 1972.
[73] ——————, Explicit formulas for Bernoulli numbers. *Amer. Math. Month.*, **79**(1972), 44—51.
[74] ——————, A new symmetrical combinatiorial identity, *J. C. T.*, A**13**(1972), 278—286.
[75] Gould, H. W. and Hsu, L. C. (徐利治), Some new inverse series relations, *Duke Math. J.*, **40**(1973), 885—891.
[76] Greene, C., On the Möbius algebra of a partially ordered set. *Adv. Math.*. **10**(1973), 177—187.
[77] Hall, M., Combinatorial theory, Blaisdell, 1967.
[78] Harary, F. and Palmer, E. M., The power group enumeration theorem, *J. C. T.*, **1**(1966), 157—173.
[79] ——————, Graphical enumeration. New York, Akad. Pr., 1973.
[80] Harrison, M. A. and High, R. G., On the cycle index of a product of permutation groups, *J. C. T.*, **4**(1968), 277—299.
[81] Harrison, M. A., Counting theorems and their applications to



classification of switching functions, in "Recent developments in switching theory". Mukhopadhyay ed., Academic Pr.. 85—120, 1971.

[82] ——————, On the number of classes of binary matrices, *IEEE Trans. Comput.*, **22**(1973), 1048—1052.

[83] Hartfiel, D. J., A lower bound on the permanent of a (0,1)-matrices, *Proc. Amer. Soc.*, **39**(1973), 83—85.

[84] Hayman, W. K., A generalization of Stirling's formula, *J. Reine Angew. Math.*, **196**(1956), 67—95.

[85] Heesch, H., Untersuchungen zum Vierfarbenproblem Hochschultaschenbücher-Verlag, 1969.

[86] Henle, M., Binomial enumeration on dissects, *Trans. Amer. Math. Soc.*, **202**(1975), 1—59.

[87] Howard, F. T., Formulas for the number of binomial coefficients divisible by a fixed power of a prime, *Proc. Amer. Math. Soc.*, **37**(1973), 358—362.

[88] Ignell, E. and Schrage, L., Application of the Branch and Bound techniques to some flow shop schduling problem. *Opns. Res.*, **13**(1965), 400—412.

[89] Jackson, P. M. and Van Rees. G. H. J., The enumeration of generalized double stochastic nonnegative integer square matrices, *SIAM J. Comput.*, **4**(1975), 474—477.

[90] Jackson, P. M., The unification of certain enumeration problems for sequences, *J. C. T.*, **A22**(1977), 92—96.

[91] Jordan, C., Calculus of finite differences. Chelsea, 1965.

[92] Karpl, R., Verallgemeinerung der Stirlingschen Zahlen der 2. Art, *Arch. Math.*, **7**(1971), 19—30.

[93] Kasami, T., The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller code, *Inform. & Control*, **18**(1971), 369—394.

[94] Kasami, T. and Tokura, N., On the weight structure of Reed-Muller codes, *IEEE Trans. Inform. Theory*, **16**(1970), 752—759.

[95] Klass, M. J., A generalization of Burside's combinatorial lemma. *J. C. T.*, **A20**(1976), 273—278.

[96] Kleitman, D. J., Algorithms, Adv. Math., **16**(1975), 233—245.

[97] Kleitman, D. J. and Rothschild, B. L., Asymptotic enumeration of partial order on a finite set, *Trans. Amer. Math. Soc.*, **205**(1975), 205—220.

[98] Knuth, D. E., The art of computer programming, V. 1 Founda-



mental algorithms, 1968; V. 2 Seminumerical algorithms, 1969; V. 3 Sorting and searching. Addison-Wesley, 1973.

[99] ————, Estimating the efficiency of backtrack programs, *Math. Comp.*, **29**(1975), 121—136.

[100] Lehmer, D. H., Teaching combinatorial tricks to a computer, Proc. Symp. Appl. Math. Amer. Math. Soc., Providence, 179—193, 1960.

[101] ————, Effective enumeration methods for highly restricted permutations, in "Proc. 25th summer meeting, Canad. Math. Cong.", 103—116, 1971.

[102] Light, F. W. Jr., A procedure for the enumeration of $4\times n$ Latin rectangles, *Fibonacci Quart.*, **11**(1973), 241—246.

[103] Little, J. D. C. et al., An algorithm for the traveling salesman problem, *Opns. Res.*, **11**(1963), 72—89.

[104] Liu, C. L., Topics in combinatorial mathematics, Math. Assoc. Amer., Washington, D. C., 1972.

[105] Lloyd, E. K., Necklace enumeration with adjacency restrictions, in "Combinatorics" (Proc. British combinatorial conf.), Univ. coll Wales., 97—102, 1973.

[106] Lomnicki, Z. A., A Branch and Bound algorithm for the exact solution of the three-machine scheduling problem, *Opera. Res. Quart*, **16**(1965), 89—100.

[107] Lynch, J. F., An asymptotic formula for the number of classes of sets of n indistinguishable elements, *J. C. T.*, A19(1975), 109—112.

[108] MacWilliams, F. J. et al., Generalizations of Gleason's theorem on weight enumerators of self-dual codes, *IEEE Trans. Inform. Theory*, **18**(1972), 794.

[109] Malloms, C. L. and Sloane, A., Weight enumerators of self-orthogonal, *Discrete Math.*, **9**(1974), 391—400.

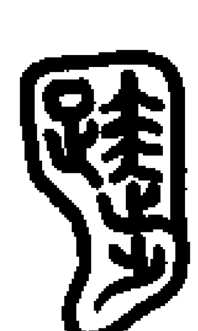
[110] Marcus, M. and Minc, H., Permanents, *Amer. Math. Month.*, **72**(1965), 577—590.

[111] Meersman, R. C., A survey of techniques in applied computational complexity, *J. Comp. Appl. Math.*, 1(1975), 33—46.

[112] Moser, L. and Wyman, M., An asymptotic formula for the Bell numbers, *Trans. Roy. S. Canada*, **49**(1955), 49—54.

[113] ————, Stirling numbers of the seconde kind, *Duke Math. J.*, **25**(1958), 29—43.

[114] ————, Asymptotic development of the Stirling numbers of first kind, *J. London Math. Soc.*, **33**(1958), 133—146.



[115] Nabeshima, I., The order of n items processed on m machines (III), *J. Opn. Res. Soc. Japan*, **16**(1973), 131—150.

[116] Nash-Williams and Sheehan, J. ed., Proc. 5th British combinatorial conf., Utilitas Math. Pub. Inc., 1976.

[117] Neufeld, G. A. et al., Graph colouring condition for the existence of solutions to the timetable problem, *Comm. ACM*., **17**(1974), 450—453.

[118] Nijenhuis, A. and Wilf, H. S., Combinatorial algorithms, Academic Pr., 1975.

[119] Niven. I., Formal power series, *Amer. Math. Month.*, **76**(1969). 871—889.

[120] Nivat, P., Sorting of permutations, in "Permutations" (Actes colloq., Paris), 251—256, 1972.

[121] O'Neil, P. E., Asymptotics and random matrices with row-sum and column-sum restrictions, *Bull. Amer. Math. Soc.*, **75**(1969), 1276—1292.

[122] Ore, O., The four-colour problem. New York Academic, 1967.

[123] Park, J. H. Inductive proof of an important inequality, *IEEE Trans. Inform. Theory*, **15**(1969), 618.

[124] Parthasarathy, K. R. and Sridharan. M. R., On structure enumeration theory, *Indag Math.*, **33**(1971), 327—339.

[125] Percus, J. K., A note on extension of the Lagrange inversion formula, *Comm. Pure Appl. Math.*, **17**(1964), 137—146.

[126] ————, Combinatorial methods, Springer, 1971.

[127] Pólya, G., Kombinatorische Anzahlbestimmunge für Gruppen. Graphen und chemische Verbidungen, *Acta Math.*, **68**(1937), 145—254.

[128] Pólya, G. and Szegö, G., Problems and theorems in analysis, V, 1, V. 2, Springer, 1976.

[129] Рыбников, К. А., Введение в комбинаторный анализ, М. Изд.-Во МТУ, 1972.

[130] Rademacher, H., Lectures on elementary number theory, 1964.

[131] Read, R. C., Some recent results in chemical enumeration, in "Proc. conf. Western graph theory and application, Michigan Univ.", Springer, 243—259, 1972.

[132] Riordan, J., An introduction to combinatorial analysis, Wiley, 1959.

[133] Robinson, R. W., Enumeration of coloured graphs, *J. C. T.*, **4** (1968), 181—190.

[134] Ronald, A., How many Latin squares are there? *Amer. Math.*



Month., **82**(1975). 632—634.

[135] Rota, G. C., On the foundations of combinatorial theory I: Theory of Möbius functions, Z. F. Wahrscheinlich Keitsrechung, 2 (1964), 340—368.

[136] ——————, Generalized Pólya theory, Seminar notes, ed. by D. Smith. Duke Univ., 1969.

[137] ——————, On the combinatorics of the Euler characteristic, Studies in pure math, ed. by Mirsky, Acad. Pr., 1971.

[138] Rothaus, O. S., Study of the permanent conjecture and some generalization, *Bull. Amer. Math. Soc.*, 78(1972), 749—752.

[139] Ryser, H. J., Combinatorial mathematics, Carus Math., 1963.

[140] Saaty, T. L., Thirteen colourful variations on Guthrie's four-colour conjecture, *Amer. Math. Month.*, **79**(1972). 2—43.

[141] Selmer, E. S., On the number of prime divisors of a binomial coefficent, *Math. Scand.*, **39**(1976), 271—281.

[142] Schmidt, D. C. and Druffel, L. E., A fast backtracking algorithm to test directed graphs for isomorphism using distance matrices, *J. Assoc. Comput. Mach.*, **23**(1976), 433—445.

[143] Singmaster, D., Notes on binomial coefficents. I. II, III. *J. London Math. Soc.*, 8(1974). 545—560.

[144] Sloane, N. J. A. and Berlekamp. E. R., Weight enumerator for second-order Reed-Muller codes *IEEE Trans. Inform. Theory*, **16**(1970), 745—751.

[145] Sloane, N. J. A., Handbook of integer sequences, Academic Pr., 1973.

[146] Stanley, R. P., Combinatorial reciprocity theorem, *Adv. Math.*, **14**(1974), 194—253.

[147] ——————, Binomial posets, Möbius inversion and permutation enumeration. *J. C. T.*, **A20**(1976). 336—356.

[148] Stone, H. S., A note on a combinatorial problem of Burnett and Coffman, *Comm. ACM.*, 17(1974), 165—166.

[149] Sugino, M. et al., Weight distribution of (128,64) Reed-Muller codes, *IEEE Trans. Inform. Theory*, 17(1971), 627—628.

[150] Szegö, G., Orthogonal polynomials, *Amer. Math. Soc. Coll. Pub.* Vol. XXIII, rev. ed., 1959.

[151] Takacs, L., Combinatorial methods in the theory of stochastic processes, Wiley, 1967.

[152] Tomescu, I., Introduction to combinatorics, Collet's Pub., 1975.

[153] Van Lint, J. H., Coding theory, Springer-Verlag, 1971.

[154] ——————, Combinatorial theory seminar, Springer-Verlag,



1974.

[155] Ward, H. N., A restriction on the weight enumeration of a self-dual code. *J. C. T.*, **A21**(1976), 253—255.

[156] Wells, M. B., The number of Latin squares of order eight, *J. C. T.*, **3**(1967), 98—99.

[157] White, D. E., Multilinear enumerative techniques, *Linear and multilinear algebra*, **2**(1975), 341—352.

[158] Wilf, H. S., A mechanical counting method and combinatorial applications, *J. C. T.*, **4**(1968), 246—258.

[159] Williamson, S. G., Operator theoretic. invariants and the enumeration theory of Pólya and de Bruijn, *J. C. T.*, **8**(1970), 162—169.

[160] ——————, The combinatorial analysis of patters and the principle of inclusion-exclution, *Discrete Math.*, **1**(1972), 357—388.

[161] Wright, E. M., Asymptotic relations between enumerative functions in graph theory, *Proc. London Math. Soc.*, **20**(1970), 558—572.

[162] ——————, The asymptotic enumeration of unlabelled graphs, in [116], 665—677, 1976.

[163] Yeh, R. T., Applied computation theory: Analysis design, modeling, Pretice-Hall, 1976.

(1. 本参考文献所列期刊论文部分以1970年以后出现的为主，1970年以前的工作只限于书中各章节里直接引用过的。关于1970年前的详目可见 Comtet [51].

2. 因 *Journal of Combinatorial Theory* 一刊引用较多，文中均简记成 *J. C. T.*).



名 词 索 引

（以汉语拼音为序，名词后的号码表示节次）

A

B

C

D

E

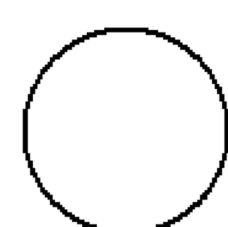
F



G

H

J



K

L

M

O

P

Q



R

S

T

V

Y



Z

